Carnegie Mellon
Software Engineering Institute

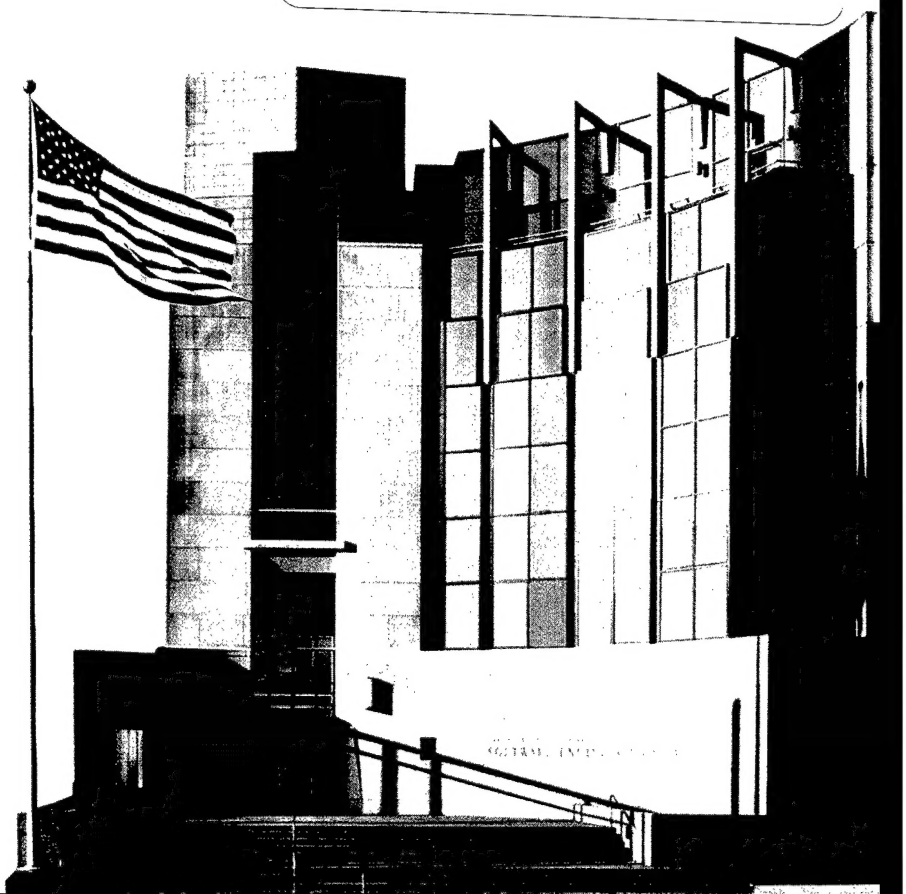
Outsourcing Managed Security Services

Authors
Julia Allen
Derek Gabbard
Christopher May

Contributors
Eric Hayes
Carol Sledge
BITS IT Service Providers Working Group

January 2003

SECURITY IMPROVEMENT MODULE
CMU/SEI-SIM-012



Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Outsourcing Managed Security Services

CMU/SEI-SIM-012

Authors
Julia Allen
Derek Gabbard
Christopher May

Contributors
Eric Hayes
Carol Sledge
BITS IT Service Providers Working Group

January 2003

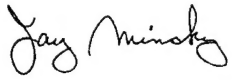
Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER



Jay Minsky
Contracting Officer's Representative

This report was developed by the Networked Systems Survivability Program at the Software Engineering Institute through funding from the General Services Administration Federal Computer Incident Response Center (GSA FedCIRC).

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our web site (http://www.sei.cmu.edu/publications/pubweb.html).

Acknowledgements

The authors would like to thank Sheila Rosenthal, reference librarian at the Software Engineering Institute, for identifying and obtaining pertinent source material and securing copyright permissions.

The authors would also like to thank those who provided sample service-level language and reviewed this report for their insight, support, and substantive comments; their efforts greatly enhanced this report

C. Warren Axelrod	BITS IT Service Providers Working Group; Pershing: a Division of Donaldson, Lufkin & Jenrette Securities Corporation, a CSFB Company
Faith Boettger	BITS IT Service Providers Working Group; BITS
Nick Brigman	RedSiren Technologies
Roopangi Kadakia	FirstGov, Office of Citizen Services & Communication, General Services Administration
Al Leary	RedSiren Technologies
Ray Lewis	Cisco
Alan Meyer	BITS IT Service Providers Working Group; Harris Bankcorp
Kevin Nixon	Exodus
Kathleen Powers	RedSiren Technologies
Gary Todd	United States Secret Service
George Vrabel	BITS IT Service Providers Working Group; Bank of America
Amit Yoran	Symantec (formerly Riptech)

Software Engineering Institute:
Rich Caralli
Klaus-Peter Kossakowski
Bradford Willke
William Wilson
Carol Woody

Table of Contents

Outsourcing Managed Security Services

As computer attack patterns shift and threats to networks change and grow almost daily, it is critical that organizations achieve reliable information security. Investment decisions about information security are best considered in the context of managing business risk. Risks can be accepted, mitigated, avoided, or transferred. Outsourcing selected managed security services (MSS) by forming a partnership with a Managed Security Service Provider (MSSP) is often a good solution for transferring information security responsibility and operations. Although the organization still owns information security risk and business risk, contracting with an MSSP allows it to share risk management and mitigation approaches.[1]

More and more organizations are turning to MSSPs for a range of security services to reduce costs and to access skilled staff whose full-time job is security. Such services may include

- network boundary protection, including managed services for firewalls, intrusion detection systems (IDSs), and virtual private networks (VPNs)
- security monitoring (may be included in network boundary protection)
- incident management, including emergency response and forensic analysis. (This service may be in addition to security monitoring.)
- vulnerability assessment and penetration testing
- anti-virus and content filtering services
- information security risk assessments
- data archiving and restoration
- on-site consulting

Managed security services is one of the fastest growing market segments in the security marketplace according to Gartner, a research and IT consulting company. In terms of some reported market trends, Gartner reports that by 2005, 60 percent of enterprises will outsource the monitoring of at least one network boundary security technology [Pescatore 02]. The META Group, also a research and IT consulting company, expects to see maturity first in the managed VPN and firewall arenas. MSS-based vulnerability scanning is forecast to mature next (2003), followed by intrusion detection (2003 - 2004), security monitoring and response (2004), and authentication and administration (2004 - 2005) [King 01]. According to IDC, a division of the research and technology company International Data Group (IDG), by 2004 security services are expected to become a $16.5B industry with a 35 percent compound annual growth rate [Navarro 01].

[1] Said differently, business risks can result when information assets upon which the business depends are not securely configured and managed (resulting in asset compromise due to violations of confidentiality, availability, and integrity). Business risk can be mitigated by lowering the probability of information security risks. Information security risks can be mitigated by having more secure information assets. More secure information assets can be achieved by satisfying security requirements. Specific security requirements can be satisfied by using managed security services, competently delivered.

Organizations need high quality strategic and practical guidance about how to work with these emerging companies to maximize their own information security. This includes well-defined practices to evaluate, select, contract with, manage, and terminate relationships with MSSPs.

The range of services offered by MSSPs varies in their ability to meet an organization's security requirements, including the availability, confidentiality, and integrity of information assets critical to the organization's mission. Therefore, it is vital that an organization specify its security requirements and require candidate MSSPs to demonstrate their ability to meet them, both as part of evaluation and selection and while providing ongoing services.

An organization needs to understand the level of information security risk in outsourcing any managed security service when developing the Request for Proposal (RFP). The costs to procure, operate, and manage provider service delivery, including review for compliance with the Service Level Agreement (SLA) and the overall contract, should not exceed the anticipated benefit.

Benefits of Engaging an MSS Provider

The results from engaging a reputable, competent MSSP have the potential to be far superior to anything an organization can achieve on its own. Described in this section are reasons for contracting with a MSSP and some of the benefits that may result from the relationship. All of these factors can contribute to reducing the risks faced by the client through a combination of risk mitigation and risk/liability sharing between the client and the MSSP [Navarro 01].

Cost

The cost of a managed security service is typically less than hiring in-house, full-time security experts [Wilbanks 01]. An MSSP is able to spread out the investment in analysts, hardware, software, and facilities over several clients, reducing the per client cost [Hulme 01]. As one example, an MSSP claims it can set up and monitor security on a 250-user network on a single T1 (1.5 Mbps) Internet gateway for about $75,000 a year, excluding hardware. Replicating these actions within the organization produces similar hardware costs, plus at least $240,000 in annual compensation to hire three full-time specialists, based on data from the magazine InformationWeek's most recent Salary Survey[2] [Hulme 01]. A client organization can convert variable costs (when done in-house) to fixed costs (services), realize a tax advantage by deducting MSSP fee expenses from current year earnings versus depreciating internal assets, and experience cash flow improvements resulting from the transfer of software licenses (and possibly personnel) to the MSSP [Alner 01].

[2] http://www.informationweek.com/benchmark/advisor

Staffing
A shortage of qualified information security personnel puts tremendous pressure on IT departments to recruit, train, compensate, and retain critical staff [Hulme 01]. The cost of in-house network security specialists can be prohibitive [Wilbanks 01]. When outsourcing, the costs to hire, train, and retain highly skilled staff becomes an MSSP responsibility. An MSSP is likely to retain security experts by offering a range of career opportunities and positions from entry level to senior management, all within the information security field [Navarro 01]. In addition, if a client organization can outsource repetitive security monitoring and protection functions, then they can then focus internal resources on more critical business initiatives [Pescatore 01a].

Skills
An in-house staff member who only deals with security on a part-time basis or only sees a limited number of security incidents is probably not as competent as someone who is doing the same work full-time, seeing security impacts across several different clients, and crafting security solutions with broader applicability [Hulme 01].

MSSPs have insight into security situations based on extensive experience, dealing with hundreds or thousands of potentially threatening situations every day, and are some of the most aggressive and strenuous users of security software [Navarro 01, DeJesus 01].

Facilities
MSSPs can also enhance security simply because of the facilities they offer. Many MSSPs have special security operations centers (SOCs) located in various parts of the country. These are physically hardened sites with state-of-the-art infrastructure managed by trained personnel. [DeJesus 01]

Objectivity and Independence
An organization may have multiple, ad hoc solutions to handle the same types of security problems. There may be no enterprise-wide management of security or of strategy. Moving security to a capable security service provider may help simplify and strengthen the enterprise's security posture [DeJesus 01]. An MSSP can provide an independent perspective on the security posture of an organization and help maintain a system of checks and balances with in-house personnel. An MSSP can often provide an integrated, more coherent solution, thereby eliminating redundant effort, hardware, and software.

Security Awareness
It is difficult for an organization to track and address all potential threats and vulnerabilities as well as attack patterns, intruder tools, and current best security practices. An MSSP is often able to obtain advance warning of new vulnerabilities and gain early access to information on countermeasures. An MSSP can advise on how other organizations handle the same types of security problems. [Alner 01, Navarro 01]

An MSSP is likely to have contact with highly qualified and specialized international security experts as well as other MSSPs. These resources can be brought to bear to diagnose and resolve client issues.

Prosecution
The MSSP are often well connected to law enforcement agencies around the world and understands what forensic analysis and evidence are required to successfully support legal proceedings.

Service Performance
When an organization contracts for security monitoring services, the service can report near real-time results, 24 hours a day, 7 days a week, and 365 days a year. This is a large contrast with an in-house service that may only operate during normal business hours. MSSPs can be held accountable for the service standards they provide. They guarantee service levels and assure their availability; failing to do so can have financial repercussions.

Their operational procedures are designed to ensure uninterrupted service availability. Also, if the MSSP is providing service systems, then it is their responsibility to upgrade software and hardware and to maintain a secure network configuration. Because MSSPs have strict contractual obligations to their clients and must maintain their reputation in the marketplace, their control procedures are generally both well documented and carefully enforced [Alner 01]. In all instances, the client needs to verify these performance characteristics.

Service Security and Technology
Service security solutions and technologies such as firewalls, intrusion detection systems (IDSs), virtual private networks (VPNs), and vulnerability assessment tools are far more effective because they are managed and monitored by skilled security professionals. For example, when an intrusion is detected, MSSPs can use a remote monitoring connection to determine whether the alarm is justified and block further intruder actions. A managed service can protect the client's network from unsecured VPN endpoints [Wilbanks 01]. For products developed by the MSSP and used in their services, the client organization receives an enhanced level of product support [Navarro 01].

The MSSP may use other third party provider products as the basis for providing service (such as firewalls and IDSs). Based on the size of the MSSP's client base, the MSSP may be able to influence the product provider to improve the security of their products by, for example, addressing new attacks and vulnerabilities.

Risks in Engaging an MSS Provider

While an MSSP may have more competent staff to manage security services, they may not be as effective in applying remedies that meet the specific needs of the client. MSSPs sometimes run the risk of applying solutions that are too generic to benefit the client. Also, sometimes the client's staff is more adept at providing the best solution.

In deciding to engage an MSSP, an organization needs to treat the potential action as a risk mitigation sharing decision. Regardless of an MSSP's role, the client is responsible for addressing the impact of a risk that has become a reality. The client must always be prepared to manage and respond to manifested risks.

There are counter arguments and issues to consider when weighing the risks against the benefits described above. Some of these include the following:

Trust
The challenge of establishing a good working relationship and building trust between a client and MSS provider remains as a significant hurdle in deciding to outsource security services. Any MSSP has access to sensitive client information and details about the client's security posture and vulnerabilities. The intentional or inadvertent public release of such information can be extremely damaging to the client. A signed confidentiality agreement enacted in the later stages of contract negotiations can help mitigate this risk.

Dependence
An organization can become operationally dependent on a single MSSP and be greatly affected by the MSSP's business viability (refer to Practice 1, P1.1 Business Attributes), other clients, and business partnerships. One risk mitigation approach is to outsource to multiple providers, but this comes with additional cost and management oversight responsibilities. An organization needs to carefully examine the provider's proposal to understand whether they use tiered providers and how they work. (Tiered providers are the subcontractors used by the MSSP and any other downstream subcontractors .) Organizations must ensure that both the client and provider have the necessary and contractual checks and balances with respect to tiered provider performance.

Ownership
A client retains ownership and responsibility for the secure operation of its infrastructure and the protection of its critical assets regardless of the scope of services provided by an MSSP. An organization may start to ignore pressing security issues due to "out of sight, out of mind" thinking, having delegated this concern to the provider. The client must ensure that it retains sufficient competency to fulfill its responsibility and that contractual and service level agreement language supports this. Risk mitigation approaches include making information security the primary responsibility for one or more staff members and managers and conducting regular user security awareness and training sessions.

Shared Environment
The shared operational environment used by many MSSPs to service multiple clients poses more risks than an in-house environment. Sharing a data transmission capability (such as a common network) or a processing environment (such as a general purpose server) across multiple clients can increase the likelihood of one organization having access to the sensitive information of another.

Implementation
Initiating a managed security services relationship may require a complex transition of people, processes, hardware, software, and other assets from the client to the provider or from one provider to another, all of which may introduce new risks. IT and business environments may require new interfaces, approaches, and expectations for service delivery. Roles and responsibilities are often redefined. [Ambrose 01]

Clients should ask for an implementation timeline and duration as well as a high-level implementation plan as part of a provider's proposal.

Partnership Failure
One of the greatest risks comes from inadequate, incomplete planning and infrequent communication and review between the provider and the client. This partnership can fail at any stage. Like any business relationship, it requires attention, care, and due diligence.

Hidden Costs and Impacts
Certain costs are overlooked or ignored because they are difficult to quantify. An organization needs to factor these into its risk analysis and decision-making processes before engaging an MSSP. Some of the hidden costs and areas where issues could arise are listed below. [Ott 01]

- Costs associated with giving up control (experience, knowledge, skill development associated with) of critical assets and security technologies
- What happens at the end of the contract period? What happens if the original provider goes out of business, delivers poorly, or is more expensive when the contract is recompeted? What is the cost of switching to a new provider?
- Would an MSSP do the job with the same quality and thoroughness that an organization would do for itself?
- How are needs met and services provided for multiple clients and how are they prioritized by the MSSP?

Legal Issues
An organization and an MSSP need to evaluate and discuss potential legal issues that could arise during a security incident involving both parties. The client needs to understand the jurisdiction under which the provider operates, the applicable laws and regulations, whether or not these laws apply to the client when engaging provider services, and if so, if these laws are compatible with the client's operation and acceptable to the client. This applies to tiered providers as well.

How to Use These Practices

The practices recommended in this report provide organizations with the guidance necessary to knowledgeably engage MSSPs, so they can make informed use of such services. Readers should view all practice guidelines as a baseline checklist from which to choose and create their own set, based on their organization's business objectives and desired security services.

These practices are intended primarily for those responsible for the selection and day-to-day oversight of outsourced managed security services. This may include your chief information officer, chief financial officer, contracting/purchasing manager, information technology manager, chief security officer, and technical staff (system and network administrators) responsible for ensuring MSSP performance and compliance with requirements.

These practices do not cover

- the enterprise business risk evaluation and accompanying decision to outsource selected security services and engage an MSSP
- expanding and renewing outsourced security services
- dealing with an MSSP being acquired by another company or going out of business
- MSS consulting services such as security architecture development and implementation, risk assessments, and forensic investigations. These services typically rely heavily on specific business objectives and processes.
- business, technical, and contractual considerations beyond those for engaging a MSSP so as to ensure client information security. However, some of these aspects are discussed briefly, in the context of the practice where they are described.

These practices assume that the client organization has made a well-informed business decision to outsource specific security services and understands the risks inherent in doing so. To knowledgeably select, engage, manage, and terminate MSSP relationships and the services they provide, we recommend a three-step approach. It requires implementing security practices in three general areas:

1. Engaging an MSS provider
2. Managing the relationship with an MSS provider
3. Terminating an MSS provider relationship

The first practice in Engaging an MSS Provider provides content guidance for an MSS Request for Proposal (RFP). The RFP establishes the client's requirements that need to be addressed in a provider's proposal. The second practice describes guidelines for evaluating a provider's proposal beyond those implied by the RFP guidelines. The third practice provides content guidance for an MSS Service Level Agreement (SLA). The SLA is one part of the contract between client and provider. It addresses some of the RFP requirements.

We divide SLA guidelines into two categories: service-specific agreements and operational security practice agreements. The service-specific agreements address characteristics and attributes of the service being provided. The operational security practice agreements address the quality of the operational security environment in which the services execute. This latter set of content guidance (titled Security Practices) does not typically appear in today's SLAs but represents critical content upon which client and provide agreement should occur.

Managing the Relationship with an MSS Provider includes guidelines for establishing a new provider relationship, transitioning from in-house services to provider-supplied services, or transitioning from one provider to another. The second practice in this area addresses the ongoing client/provider relationship.

Finally, we list guidelines to consider using when an organization terminates a relationship with an MSSP, whether at the end of a contract or for some other reason.

In addition, we provide two service-specific practices that provide more detailed guidelines to consider when outsourcing network boundary protection services and vulnerability assessment services.

Summary of Recommended Practices

Area	Recommended Practice
Engagement	1. Content Guidance for an MSS Request for Proposal 2. Guidance for Evaluating an MSS Proposal 3. Content Guidance for an MSS Service Level Agreement
Management	4. Transitioning to MSS 5. Managing an Ongoing MSS Provider Relationship
Termination	6. Terminating an MSS Provider Relationship
Service-specific	7. Considerations for Network Boundary Protection as Managed Security Services 8. Considerations for Vulnerability Assessment as a Managed Security Service

In the Engagement practices (Practices 1, 2, and 3), we have organized guidelines in sections titled Business Attributes, Service Attributes, and Security Practices. In financial and security communities, these are sometimes referred to as security controls and serve as the means by which an organization or service is evaluated for compliance with requirements. This is done by verifying the presence, absence, or degree of implementation of specific attributes and practices.

Attributes and practices are generally presented in order of priority but may need to be re-ordered and tailored to meet specific business and MSS objectives. Where applicable, each attribute and practice should be a table of contents entry in an RFP, on a proposal checklist when evaluating provider proposals, and a table of contents entry in the SLA.

Each attribute and practice should be addressed during transition (Practice 4), ongoing management and review (Practice 5), and considered when terminating a provider relationship (Practice 6). The service-specific guidelines presented in Practices 7 and 8 assume the attributes and security practices presented Practices 1, 2, and 3.

When taken in their entirety, we recognize that following these practices may seem overwhelming from both a client and provider perspective. In addition, they may result in spending more to protect an information asset than is warranted based on the asset's value and risk of compromise. This may be particularly the case for smaller organizations that do not have the level of staffing or the expertise to accomplish these guidelines. Making well informed and tailored selections is key to a successful contract and client/provider relationship.[3]

These practices were developed in collaboration with the BITS IT Service Providers Working Group. They draw extensively from the *BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships, Version 3.2a,* published August 17, 2001 and approved by the BITS Board of Directors in October, 2001 [BITS 01].

Terminology

For the purposes of this report, we use the following terms as defined below:

- Client – an organization interested in purchasing security services from a managed security services provider
- Provider – the MSSP, vendor, or supplier of such service
- Tiered provider – a subcontractor of the primary provider
- Business attributes, service attributes, security practices – also known as security controls in the financial and security communities, to connote the means by which an organization or service is evaluated for compliance with requirements. See the Acronyms section below for a list of these controls.
- Information asset – something of value to the provider or to the client. Information technology assets include information, systems, networks, software, hardware, and can include people (such as key staff members). Critical assets are the most important assets to a client or provider, such that the enterprise will suffer a large adverse impact if something happens (violations of confidentiality, availability, or integrity) to one of these assets. [Alberts 01a]
- Attack – an action conducted by an adversary, the attacker, against a potential victim. A set of events that an observer believes to have information assurance consequences for some entity; the target of the attack. From the perspective of an administrator responsible for maintaining a system, an attack is a set of one or more events that has one or more security consequences. From the perspective of a neutral observer, the attack can either be successful (an intrusion), or unsuccessful (an attempted or failed intrusion). From the perspective of an intruder, an attack is a mechanism to fulfill an objective. Intrusion implies forced entry, while attack only implies the application of force. [Allen 00]

[3] Meta Group [Raffoul 02] proposes one structure that they call an outsourcing management maturity model. This model consists of five levels (vendor management fundamentals, defined service outcome, measurement, trust, recognized business value) that order a reasonable set of practices to mature an outsourcing relationship.

- Incident – a collection of data representing one or more related attacks. Attacks may be related by attacker, type of attack, objectives, sites, or timing. [Allen 00]
- Intrusion – actual illegal or undesired entry into an information system. The act of violating the security policy or legal protections that pertain to an information system. [Allen 00]

Acronyms

BC/DR	Business Continuity/Disaster Recovery
DMZ	Demilitarized Zone
GRT	Guaranteed Response Time
IDS	Intrusion Detection System
IT	Information Technology
ISP	Internet Service Provider
Mbps	Megabits per second
MSS	Managed Security Services
MSSP	Managed Security Service Provider
NFPA	National Fire Protection Association
RFP	Request for Proposal
ROI	Return on Investment
SLA	Service Level Agreement
SOC	Security Operations Center
VA	Vulnerability Assessment
VPN	Virtual Private Network
WORM	Write Once, Read Many

Business Attributes

AO	Asset Ownership
CE	Contractual Exceptions, Penalties, and Rewards
CS	Client Satisfaction
ES	Exit Strategy
IE	Independent Evaluations
IP	Implementation Plan
PC	Points of Contact
PR	Personnel
RO	Relationships with Other Parties
SA	Service Level Agreement
SV	Site Visit
VI	Viability

Service Attributes

CO	Cost
HS	Service Hardware and Software
RR	Reporting Requirements
SP	Service Scope
SL	Service Levels
SR	Top-level Security Requirements
SS	Service Scalability
ST	Service Architecture
SY	Service Availability

Security Practices

AA	Authentication and Authorization
AC	Access Control
BU	Backups
DH	Data Handling
DR	Contingency Planning; Operational and Disaster Recovery
IM	Incident Management
MA	Monitoring and Auditing
PP	Security Policies, Procedures, and Regulations
PS	Physical Security
SC	Secure Asset Configuration
SI	Software Integrity

Practice 1: Content Guidance for an MSS Request for Proposal

The Managed Security Services (MSS) Request for Proposal (RFP) is intended to elicit proposals from qualified Managed Security Service Providers (MSSPs) with the skills and experience to meet a client's security service requirements. In addition to a clearly defined statement of work describing the desired services, the RFP should identify all requirements the provider's offering is expected to satisfy. This includes business attributes and service attributes to ensure that both the client and provider are satisfied with the level of contracted service, as well as the security practices that the client expects the provider to deploy in the operational security service environment. The presence of such practices instills confidence that the provider is running a secure operation, can successfully protect client data, and is "practicing what it preaches."

MSS RFP requirements are based upon the anticipated relationship with the provider and the service(s) to be provided. The client should design the RFP to reflect its security policies and expect providers to provide responses that outline cost-effective services that comply with these policies.

If feasible, consider soliciting proposals from in-house IT teams. "Including internal teams creates a more competitive environment because suppliers must demonstrate value beyond what is available in-house." [Lacity 02] "Research shows that customers who invited internal IT teams to compete with external suppliers made successful sourcing decisions 83 percent of the time. Customers who did not invite in-house bids but only compared existing costs to one or two supplier bids had only a 42 percent success rate." [Lacity 01, Lacity 02]

Instruct the provider to include any requirements defining client roles and responsibilities that will help ensure a successful partnership. This applies to business attributes (P1.1), service attributes (P1.2), and security practices (P1.3).

In an RFP, a client should ask providers to indicate any ways in which they are unable to comply with a specific requirement. Conflicts could exist because of regulations, legal requirements, policies, or other considerations. If the provider cannot comply with one or more of the requirements, they should offer alternatives, if possible.

When developing the RFP, a client needs to understand their level of risk in outsourcing any managed security service (see the Introduction). Understanding risks help a client to ensure that the costs to procure, operate, and manage provider service delivery, as well as the costs to ensure compliance with the Service Level Agreement (SLA), do not exceed the anticipated benefit.

P1.1 Business Attributes

Business attributes are one element of client requirements. They comprise characteristics, policies, processes, and procedures that need to be described in a qualified RFP response and include

- Viability (VI)
- Client Satisfaction (CS)
- Relationship with Other Parties (RO)
- Independent Evaluations (IE)
- Personnel (PR)
- Asset Ownership (AO)
- Contractual Exceptions, Penalties, and Rewards (CE)
- Service Level Agreement (SA)
- Exit Strategy (ES)
- Site Visit (SV)
- Implementation Plan (IP)
- Points of Contact (PC)

Some of the guidelines for eliciting provider business attributes are presented below as a series of topical questions. It may be helpful for a client to convert these questions into a checklist. If specific responses are required, turn the questions into imperative requirements statements. The pronouns "you" and "your" in the questions below refer to the provider organization. "We," "us," and "our" refer to the client organization.

P1.1.1 Viability (VI)

Viability guidelines are organized into six categories:

- VI1: Financial
- VI2: Services Offered
- VI3: Organizational Breadth
- VI4: Investment Strategies
- VI5: References

VI1: Financial

a. Provide your most recent annual report and financial statement and those of your key investors if they are not publicly available.
b. Indicate the total number of active security service contracts, indicating the percentage of multi-year and single year contracts. Describe your annual rate or percentage of new, renewing, and terminating contracts.
c. Provide information regarding any recent mergers and acquisitions, initiated by your organization or initiated by others.

VI2: Services Offered

a. Name the markets or industries you target for each of the services you offer [Cisco 01].
b. Describe what percentage of annual revenue for the previous fiscal year derives from each requested service. Indicate the number of service engagements, by requested service, which your company has conducted for clients over the past year. Indicate the average size of the client's network (small, medium, large). For example, state "Vulnerability assessment services: 10, Large." [Cisco 01]
c. What percentage of your staff is involved in direct service delivery and managing current client accounts?

VI3: Organizational Breadth

a. Is your current business (including your channel (reseller) partnerships) regional, national, or international? Describe your approach and your capabilities to provide global support, including, but not limited to, worldwide locations, expertise in national languages, knowledge of national and local laws that affect requested services, and relationships with national and local law enforcement agencies.

VI4: Investment Strategies

a. Describe your approach for investing in technology and research and development to increase operational efficiency while keeping up with the rapidly changing threat environment. What are the highest priority initiatives in your company that affect the requested services? What is your company's vision and direction for currently offered services as well as plans for additional services and support of new technologies? [Cisco 01]

VI5: References

a. Provide three references from clients
   - with similar types of organizations (size, market segment)
   - with similar levels of infrastructure complexity and capacity requirements
   - that are currently using the services requested in this RFP

Include, for each reference: the company name, contact name, contact title, phone number, email address, types of service, and dates of service. [Cisco 01]

P1.1.2 Client Satisfaction (CS)

CS1: Describe your process and mechanisms for handling client inquiries and reported problems.

CS2: Describe customer service responsiveness, hours of staff availability, and available communication mechanisms (e.g., written, verbal, electronic, face-to-face).

CS3: Describe how you measure and report client satisfaction, including frequency.

CS4: Describe how satisfaction deficiencies are addressed and resolved (in your service level agreement or elsewhere).

CS5: Describe secure communications mechanisms (e.g. secure voice, fax, encrypted email, pager) to use when communication should be private.

CS6: Include both national and international service support.

P1.1.3 Relationships with Other Parties (RO)

RO1: Provide a complete list and brief description of your channel partners, resellers, vendors, subcontractors, and other providers (tiered providers including ISPs) who may be involved in delivering the requested services. Describe your due diligence process for engaging in these types of business relationships.

RO2: Where do you plan to use tiered providers to satisfy client requirements? In what capacity do you plan to use them? What mechanisms are in place to allow the client to verify that these requirements are met? Requirements include business attributes (P1.1), service attributes (P1.2), and security practices (P1.3).

RO3: Indicate how our requirements flow to all involved tiered providers and how requirements satisfaction is determined.

RO4: The client identifies any requirements or restrictions they have when outside parties (providers, tiered providers) connect to their network. These may include: disallowing certain protocols, requirements for or restrictions on communications or encryption methods, confidentiality requirements, and specific storage requirements for security data. The provider indicates how they plan to meet these requirements and restrictions. [conversations with RedSiren]

RO5: How can we establish a direct relationship (either informal or contractual) with your tiered providers when they are involved in delivering the requested services? Indicate if we are free to contact these organizations and, if so, provide contact information.

RO6: When client information is shared with and used by tiered providers, what procedures do you have in place for protecting this information?

RO7: How are security risks associated with tiered providers defined and monitored?

RO8: What security research organizations do you partner with to stay informed about new threats and vulnerabilities?

RO9: Describe any user groups associated with requested services and describe your practice of communicating with clients through such groups.

P1.1.4 Independent Evaluations (IE)

Address these aspects of independent evaluations for the provider and for all tiered providers who deliver requested services.

IE1: Describe how you assess and manage risks to information security, periodically and in response to major changes in technology, internal and external threats, or your systems and operations. This includes regularly conducting information security risk evaluations or contracting with an outside organization to perform them. Describe how relevant results from risk assessment and management activities are communicated to the client.

IE2: Identify internal and external service risks that could lead to unauthorized disclosure, misuse, alteration, or destruction of client and client customer information assets. Describe your risk mitigation approach.

IE3: Identify the third party organization(s) responsible for conducting your latest security risk evaluation, security audit, and vulnerability assessment. Describe how often this is done and how it is performed. Include the most recent results and the date of these results.

IE4: Indicate if we are free to contact the evaluating organization(s) and, if so, provide contact information.

IE5: Indicate your agreement to participate in and deliver results from a periodic full security evaluation performed by a mutually agreeable independent organization [Alner 01]. Recent results that you provide may serve in lieu of this requirement. Do you require or obtain independent evaluations from your tiered providers? Are you willing to share these evaluations with us?

IE6: If applicable, demonstrate service compliance with or recent audit results for relevant national regulations and international standards such as the U.S. Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, ISO 17799 Information technology – Code of practices for information security management, and Statement on Auditing Standards (SAS) No. 70, Service Organizations.4

P1.1.5 Personnel (PR)

PR1: How do you screen potential employees? Describe the level of background checks performed by job position (role, responsibility, authority), particularly for positions handling sensitive client information. State your policy on hiring those with an established history of successfully breaking into computers (often referred to as hackers).

PR2: For key personnel who will provide services specified in this RFP, how many years of experience do they have and in what fields? Include resumes for key personnel and for key executives and managers who will have oversight responsibility for this contract.

PR3: Provide organizational and staff member accreditations and certifications in networking elements, security, operating systems, auditing, and evaluation [Radcliff 00]. Describe how these credentials will be used to provide the requested service.

PR4: What professional (post degree) training and certifications do your security analysts and SOC (Security Operations Center) personnel have? How recent are these?

PR5: What is your annual staff retention rate for key positions?

PR6: Are staff members assigned to a client as they are available or are they permanently assigned for the duration of the relationship?

PR7: Do new staff members receive initial training and do all staff members receive periodic refresher training on the provider's security policies and procedures?

---

[4]SAS 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). It is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination. Refer to http://www.sas70.com.

PR8: Determine the level of knowledge the provider needs and determine the appropriate level of authority the provider needs to access client data by answering the following questions [Alner 01]:
   a. Are selected provider staff members required to sign confidentiality or non-disclosure agreements?
   b. Are specific provider staff members (including consultants) bonded? This assumes bonding requirements and levels are specified in the provider company policy.
   c. Which provider staff member roles have privileged access to client data, software, and hardware? What is the justification for such access?

PR9: What security procedures are invoked when a provider staff member terminates their employment?

PR10: Do you require the above personnel information from your tiered providers? If so, are you willing to provide us with this information?

P1.1.6 Asset Ownership (AO)

AO1: Identify the owner of assets used in providing the service (systems, software, source code, processes, concepts, etc.). Providers either manage their own systems or manage equipment that the client owns. Client ownership may cost more in the short term, but may reduce transition issues when the relationship terminates.

AO2: Is all intellectual property created by the provider on behalf of the client and in the course of the relationship owned by the client? This includes reports, logs, audit and evaluation results, and the like. Specify any client-based or client-derived intellectual property that remains under provider ownership.

AO3: If you propose using proprietary assets (policies, processes, applications software), describe how the client is not placed at risk when the relationship terminates (with respect to continued use of these assets).

AO4: Describe all software and hardware license and patent issues that may relate to delivering requested services and how such assets are transitioned upon contract termination.

P1.1.7 Contractual Exceptions, Penalties, and Rewards (CE)

CE1: Provide your standard language for contractual exceptions, penalties, and rewards.

P1.1.8 Service Level Agreement (SL)

SA1: Provide your standard SLA.

SA2: Does your SLA allow for client-specific requirements for performance and remediation (restoration of service, customer service, response time) [Cisco 01]?

SA3: Describe client and provider responsibilities for monitoring and verifying SLA metrics.

SA4: What are the financial implications of SLA non-compliance? Include descriptions of how credits are applied to client accounts or other means of assuring clients are properly charged for the service provided vs. the service negotiated. [Cisco 01]

SA5: Describe the process by which clients may tailor or amend your SLA.

Refer to Practice 3 for additional details.

P1.1.9 Exit Strategy (ES)

ES1: Provide your standard contract termination language and provisions.

ES2: Indicate the conditions under which contract termination may occur.

P1.1.10 Site Visit (SV)

SV1: Indicate provider agreement for the client to conduct a site visit, including all physical facilities involved in service delivery such as the SOC and areas where client data are secured.

SV2: During site visits, reviews and demonstrations of provider capabilities as represented in the proposal will be verified, and additional scenarios or requirements may be examined. Any additional requirements will be communicated in writing prior to such a visit.

SV3: All expenses incurred by the provider during the site visit are the provider's responsibility [Cisco 01].

SV4: Specify any limitations or constraints on site visits.

P1.1.11 Implementation Plan (IP)

IP1: Provide your high-level implementation plan for installing and operating requested services. Include a timeline and estimated duration. Include your service transition approach, from the client or another provider, if applicable. Refer to Practice 4 for more details.

P1.1.12 Points of Contact (PC)

PC1: Identify both the primary client point of contact (identified in the RFP) and the provider point of contact (identified in the proposal) that will serve as the primary interface between the two organizations. Before drafting and releasing an RFP, it is important to decide which client contact will be responsible for coordination and dialogue with all providers submitting a proposal. This streamlines the proposal submission and evaluation processes and gives each provider a single point of entry into the client's organization.

PC2: These points of contact will likely not be the people responsible for managing the day-to-day client/provider interface once the contract is signed.

P1.2 Service Attributes

Service attributes are a second element of client requirements. They describe the quality of service to be provided and levels of service performance to be met. Service attributes include

- Top-level Security Requirements (SR)
- Service Availability (SY)
- Service Architecture (ST)
- Service Hardware and Software (HS)
- Service Scalability (SS)
- Service Levels (SL)
- Reporting Requirements (RR)

- Service Scope (SP)
- Cost (CO)

To qualify for consideration, the provider's proposal must demonstrate how the provider will ensure compliance with all service attributes during the execution of the contract.

The RFP must define service availability and performance requirements such that the client can make an effective comparison between different providers (e.g., the timeliness of critical alert reports, service uptime percentages). Service attributes are presented below as a series of topical statements and questions. A client needs to select those that are meaningful for a specific RFP.

P1.2.1 Top-level Security Requirements (SR)

SR1: The provider asserts and is able to satisfactorily demonstrate that client asset (software, hardware, data) confidentiality, availability, and integrity are assured in the process of delivering service.

SR2: Client privacy is protected to include but not be limited to identified client data, security posture, vulnerability status, and attack status.

SR3: The provider ensures that specified client data resides only in the client's designated country to satisfy local/regional data privacy laws [ISS 01].

Details of how these requirements are met are addressed in section P1.3 Security Practices.

P1.2.2 Service Availability (SY)

SY1: Client requirements for service availability are likely to be 24 hours a day, 7 days a week, 365 days a year (24x7x365) with 99+ percent uptime, measured as experienced by the client. This means that service availability is not measured and demonstrated at the individual provider service asset level (systems, networks, databases, applications, personnel, etc.), which has no meaning for the client.

SY2: Service uptime figures are determined using risk evaluation and analysis, determining the criticality of services and systems being provided. Consider the following guidelines:

a. 99 percent uptime = 87.6 hours unavailability or degraded capability per year, or 7.3 hours per month
b. 99.9 percent uptime = 8.8 hours unavailability or degraded capability per year, or approximately 44 minutes per month
c. 99.99 percent uptime = 52 minutes of unavailability or degraded capability per year, or 4.4 minutes of downtime per month
d. 99.999 percent uptime = 5.2 minutes of unavailability or degraded capability per year, or about 25 seconds per month

State a figure for the maximum acceptable period of continuous unavailability or degraded capability if this is different from the cumulative figures shown above.

Higher levels of service uptime will likely result in greater cost. The cost difference between 99.99 percent reliability and 99.999 percent can easily be tens of thousands of dollars a month [Turek 00]. Make sure that uptime and availability service levels are those required to meet business objectives, and no more. Service availability includes the provision for announced, coordinated, and scheduled down time for service (software, hardware, data) maintenance and upgrade. The provider states exclusions from the overall service availability uptime figure such as client ISP outages.

SY3: Service uptime relies on power, network connectivity, and bandwidth availability. The client may want to specify a guaranteed availability percentage for these architectural elements as well. For example, if service uptime is 99.9 percent, then power, network connectivity, and bandwidth availability should be specified at 99.99 percent.

SY4: Describe how you calculate service outage times. Address the following outage conditions [BITS 01, Section 4.4.6, p 22]:

a. regularly scheduled time periods when the service is not available
b. how additional service volume created by a new client affects both client and provider system performance and availability
c. interruptions in local/regional utility service (for example, communications, gas, electric, sewer, water)
d. how scheduled service software and hardware maintenance affect service availability, and whether or not this is acceptable

SY5: Provide historical statistics on system availability and response times for the requested service. [BITS 01, Section 4.4.2, p 21]

P1.2.3 Service Architecture (ST)

Prior to developing the RFP, the client should define architectural requirements and alternatives when the service is deployed, including such considerations as bandwidth requirements, the need for a demilitarized zone (DMZ), the location of service systems in the network, and connectivity between client and provider networks. The client can express their RFP requirements in more detail if they do so knowing the network architecture they will use.

The client can then more easily determine if proposed solutions meet the client's architecture requirements. Conversely, if the client does not have the capability to define such requirements, they can consider contracting for this support as a separate service. Regardless, the guidelines that follow presume the existence of an initial service architecture that is used as the basis for defining requirements.

The client needs to provide sufficient details about their operational environment in the RFP to allow providers to prepare responsive proposals.[5]

ST1: Describe, using text and graphics, how your services will be implemented to include, but not be limited to [Navarro 01]

a. remote administration. Service hardware and software are located on our networks. Your SOC connects to this equipment via secure means (such as VPN or dedicated lines).
b. co-location. Your security devices (such as managed firewalls and web servers) are placed within your data center. All access to and from our networks pass through your infrastructure, potentially including all Internet access. For this alternative, do you run our service on a dedicated server? If not, how are our data, systems, networks, and performance protected from exposure to other clients?
c. on-site. You offer permanent, on-site augmentation of our security staff and hardware/software.
d. physical location of all architectural assets (such as SOCs), including international locations.

ST2: How likely is it that the architecture you are designing and implementing is going to change over the short term (six to twelve months) and over the long term (one to five years)? For example, if we are creating business relationships that require extranets or other network configuration changes to accommodate new partners, how do you account for this? Can your service architecture be easily changed with minimal impact to our ongoing operations and performance?

ST3: What effect will your services have on our production network, if any? Are you able to monitor our network configuration as it exists today with no performance impact? [Navarro 01]

ST4: How do your monitoring devices, sensors, and servers affect other security equipment or software already in place at our site [Navarro 01]?

ST5: Describe how your service solution integrates with our in-house security devices and technologies. It is desirable to achieve a positive return-on-investment (ROI) on existing approaches to the extent possible. [Navarro 01]

ST6: Describe your capability and approach for managing multi-vendor equipment on the same network, if applicable to your solution.

---

[5] If the client does not have specific requirements for what services they want, how many of each they want, and their desired location (for example, IDS on four network segments, managed firewalls on two network segments), the client needs to include sufficient information for the provider to recommend a service architecture that best meets client security needs. Providing the following information helps the provider give the client more responsive recommendations [conversations with RedSiren]:

- the storage location of critical data, including the computer(s) and network segment(s) where the computer storing the data resides
- the network segments used when transmitting and accessing the data
- network topology diagram indicating
  - the computers and network segments identified above
  - the number of existing firewalls and their location
  - technical details, including computer operating systems in use and typical network throughput

ST7: How are your service systems managed?

a. Do you use the Simple Network Management Protocol (SNMP) to aid in systems management? (If so, consider these solutions carefully as some implementations contain documented vulnerabilities [CERT 02].)
b. Are your management tools hardened and secured? (Refer to P1.3.8 Secure Asset Configuration.)
c. Is the traffic between your SOC and our systems encrypted? Where do the encrypted tunnels terminate (assuming there are tunnels between the networks)?[6]

ST8: For service installation:

a. Are your service systems built and tested in a non-production (test or lab) environment? Are they built and tested in a production environment?
b. Do you install service systems at the client's convenience?
c. What is the expected client downtime for service installation? Do you require the client's network to be down for a certain number of hours or days in order to implement the new service system(s)?
d. Is there a trial period during which you provide on-site or immediate on-call support?
e. Are there any backdoors into service systems? Do you use modems for remote access administrative purposes? If so, are backdoors and modems disconnected or disabled when not in use? How is this demonstrated?

ST9: Documentation: Describe your process for keeping the following items current and making them available for client review.

a. diagrams of the service architecture for each physical site, including all hardware and software. If this does not include the network architecture and topology, then include this as a separate diagram.
b. an inventory of all service software including software developed by the provider. Describe the vendor, release levels, patch levels, and any other characteristics that distinguish the configuration.

P1.2.4 Service Hardware and Software (HS)

HS1: Describe the products, technologies, and operating systems that you use to deliver requested services. Some security service providers lock a client into a single technology, product, or operating system. They are, in essence, resellers for that configuration. The client needs to ensure that a provider can operate using a range of solutions.

HS2: Describe the products, technologies, operating systems, and architectures that you are able to monitor. Again, the provider needs to demonstrate flexibility.

HS3: Demonstrate that new products and technologies can be easily integrated into the provider's operational environment.

---

[6] The best practice is to have encrypted tunnels terminate on the service system (such as the firewall or intrusion detection sensor) at the client's site, and at the management system/console at the provider site. Most providers use "out of band" communication channels, such as separate management encrypted tunnels, to manage service systems. This is more secure but may require another Internet connection into service systems at the client's site.

HS4: Demonstrate that provider staff skills and expertise are sufficient to support service software and hardware.

HS5: Describe the practices you deploy to secure your security services software and hardware, both electronically and physically. (Refer to P1.3 Security Practices.)

P1.2.5 Service Scalability (SS)

SS1: How scalable is the provider's service to handle new client geographic locations (including international locations), growth in client business transactions and corresponding network traffic, and increasing and changing threats? (The client should provide applicable forecasts of business growth and decline.)

SS2: How much advance notice of the need for growth in service scale do you require? Are there any limitations in the rate of expansion that can be accommodated and penalty costs if forecasts expand or decrease beyond a specific range?

SS3: The client needs to provide their capacity and growth requirements for the period of contract performance that will affect requested services. This may include such projections as growth over time in number of users, network traffic (including public web site access), and the number of servers to be monitored.

P1.2.6 Service Levels (SL)

SL1: Describe the levels of available service, the features of each level, and decision criteria that a client may use to select a desirable level of service.

SL2: Propose pertinent measurements that can be expressed in client business performance terms based on provider experience with other clients.

SL3: Describe relevant measurements and measurement ranges for required work performed by the provider such as service speed, response times, and accuracy.

SL4: Describe how you demonstrate and assure the quality of the delivered service. Keep in mind that high levels of service speed and response time often come at the expense of accuracy.

Examples of how one might specify service levels include

- how to determine the appropriate service uptime level given the choices specified under Service Availability above.
- the range of intrusion response services to include analysis, internal and external communication with affected parties, collecting and protecting information including evidence, limiting the damage caused by the intrusion by containing it, eliminating all means of intruder access, returning systems to normal operation, and conducting an intrusion post mortem meeting to discuss lessons learned, implementing identified improvements such as removing vulnerabilities, and reducing the likelihood of similar attacks recurring.
- Levels of reported intrusion priority such as high, medium, and low (defined below):
    - high indicates that a system or application is no longer useable and this is having a significant impact on the business or on infrastructure security
    - medium indicates that a system or application is useable with a work around but is executing in a severely degraded mode. The business and security impact is moderate.

- low indicates that a system or application is experiencing some degraded performance and the impact to business and security is low.

With these definitions, the client and provider can negotiate a level of service and its corresponding response and price.

P1.2.7 Reporting Requirements (RR)

RR1: What standard and customized reports are included in your cost proposal? How frequently are these reports provided? Can they be provided immediately upon client request? Reports should detail, at a minimum: all policy modifications, all configuration changes, a prioritized list of security alerts, and information on new security threats including those that may require policy changes [Pescatore 01b]. Provide a range of sample reports and a description of how they are used by both the client and the provider.

RR2: Are reports available for specific network segments/devices for in-depth analysis or segment/device groups for overall trend analysis?

RR3: Describe the types of reports you typically produce to enhance our knowledge of our security posture including, but not limited to, trend analysis, performance planning, capacity planning, and analyzing the cost-effectiveness of your services.

RR4: How are reports typically delivered? Do you provide real-time access to network and system security status (often available as a secure web interface)? Do you offer timely security event and service outage reporting?

RR5: How is report confidentiality protected?

RR6: Describe your problem/action tracking system that addresses the initiation, status, and resolution of problems and action items. Indicate if you provide online access to the client to view status and history. Verify that service outages and other service level issues are tracked using this system. Provide sample reports produced by this system.

RR7: Describe the process by which we can audit any and all reports for accuracy.

RR8: Indicate your agreement to provide reports when requested that verify your compliance with contractual obligations [BITS 01, Section 4.1, p 20]. These could include

a. the accuracy of charges and invoices, including assurance and demonstration that the client cannot be billed for another client's use of provider resources [Alner 01]
b. the provider's performance related to its
    1. internal practices and procedures
    2. disaster recovery and backup
    3. efficiency and effectiveness in using resources to provide services for which the client is charged
    4. performance of the services according to performance standards

RR9: Describe the training you offer to assist the client in understanding how to access reports (for online versions), interpret them, and audit all reports.

Refer to Practice 5 for additional details about possible reports to consider.

P1.2.8 Service Scope (SP) (This content will most likely appear in Statement of Work task descriptions.)

SP1: Do your services include consulting and training? Describe available training and on-site support to operationally assist us when your services are in place as well as to address any service limitations.

P1.2.9 Cost (CO)

CO1: Provide options for service structure, levels, and costs as well as service ROI (return on investment) information. Different levels of service are generally delivered at different costs.

CO2: Indicate the basis for any changes in cost such as annual review results, comparison with industry benchmarks, service use beyond negotiated levels, etc.

CO3: Describe any cost advantages for a long term contractual commitment and if this varies by duration.

P1.3 Security Practices

Security practices are a third element of client requirements. The client must define the security policies, procedures, and resulting practices that the provider is expected to demonstrate.[7] A client must require that

- the provider's network and system infrastructure operates securely (that is, uses good, commonly accepted security practices). The provider must also require the same standards from any tiered providers with whom they subcontract.
- the client's network and system infrastructure remain well secured when the provider's service is deployed

Keep in mind that specific practice implementations vary depending on the provider's operational environment (shared vs. dedicated, single vs. multiple providers) and vary depending on the service being provided (for example, a provider's security operations center handles multiple clients and is partially outsourced to another provider).

This list of good, commonly accepted security practice topics is taken from the *OCTAVE℠ Catalog of Practices, Version 2.0.* [Alberts 01b] and the *BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships, Version 3.2a* [BITS 01].[8] A client needs to select security practices that are meaningful for a specific RFP and for a specific set of services. Practice topics include

- Security Policies, Procedures, and Regulations (PP)
- Contingency Planning; Operational and Disaster Recovery (DR)
- Physical Security (PS)
- Data Handling (DH)
- Authentication and Authorization (AA)

[7] Although we expect that some providers may not feel obliged to provide this information.

[8] Additional sources of credible, reputable practice recommendations may be found in four references found in the Bibliography of this report: [ISO/IEC 01], [Tipton 00], [ISF 01], [Allen 01].

- Access Control (AC)
- Software Integrity (SI)
- Secure Asset Configuration (SC)
- Backups (BU)
- Monitoring and Auditing (MA)
- Incident Management (IM)

P1.3.1 Security Policies, Procedures, and Regulations (PP)

PP1: The provider has a comprehensive set of documented, current policies that are periodically reviewed, updated, and enforced. These policies are available for client review.

PP2: The client provides relevant security policies as part of the RFP, including policies that specifically address the purpose and scope of the requested services. Ensure policies describe the purpose of the services and companion systems that are being requested and their responsibilities. For example, a client's security policy states that inbound connection requests to the client's internal network are not permitted from an untrusted network such as the Internet. Based on this policy, a provider can configure a firewall to block or deny all inbound packets that are not in response to requests from within the internal network.

We understand that many client organizations do not have documented security policies, procedures, and practices or that they may not be able to share them publicly. In the absence of these, the client should ask specific questions in the RFP that address areas of concern to ensure client assets will be adequately protected. Business attributes (P1.1), service attributes (P1.2), and security practices (P1.3) can serve as a candidate list of topics for formulating such questions.

PP3: Compliance:

a. The provider asserts that their security policies and procedures are compliant with those that the client has provided and do not conflict. Where compliance and conflict issues exist, the provider indicates how these are to be resolved.
b. The provider demonstrates its ability (and the ability of its tiered providers, if applicable) to meet applicable legal and regulatory requirements and the timely implementation and demonstration of compliance procedures. (The client provides these requirements in the RFP.)
c. The provider demonstrates that they are exercising an appropriate standard of due care with respect to securing information assets, primarily accomplished through security policies, procedures, and practices that are documented and enforced.

P1.3.2 Contingency Planning; Operational and Disaster Recovery (DR)

DR1: The provider has business continuity and disaster recovery (BC/DR) plans for critical assets and asserts that they are periodically tested and found effective. For example:

a. The provider has deployed operational redundancy (via a dual, high availability environment) in the event of a primary SOC failure.
b. A failover site, physically and geographically separate from the provider's primary site, exists in the event of a natural disaster (earthquake, hurricane) or other circumstances that affect business continuity such as interruptions in local/regional utility service (communications, gas, electric, sewer, water). Or, conversely, the provider operates requested services using a distributed architecture from geographically diverse locations in the event of primary site loss of power, loss of Internet connectivity, natural disasters, etc.
c. The provider contracts with multiple ISPs and is connected to multiple public exchanges operating on different trunk lines to ensure no loss of Internet connectivity.

DR2: The provider's plan describes [BITS 01, Section 4.12, p 24]

a. access control requirements under disaster response mode involving a provider site outage
b. the differences, if any, in access controls between operational and disaster recovery scenarios

DR3: The provider provides a copy of their BC/DR plan and procedures applicable to the requested services and the site(s) where these services are operated.

DR4: The provider indicates if BC/DR testing is certified by an independent third party and, if so, provides a copy of the certification. [BITS 01, Section 4.12, p 24]

DR5: The provider provides a copy of recent (within the last year) BC/DR test results.

DR6: The provider's BC/DR plans and testing of these plans includes all tiered providers involved in delivering the requested services.

DR7: The provider (and any tiered providers involved) can support periodic joint testing of both the client's and provider's BC/DR plans. Such joint tests include impact scenarios that could potentially cause unacceptable interruption to client services. [BITS 01, Section 5.11.2, p 33]

DR8: The provider demonstrates compliance with NFPA (National Fire Protection Association) 1600 - Standard for Disaster/Emergency Management and Business Continuity Programs.[9]

[9] Information on this standard is available at http://www.davislogic.com/NFPA1600.htm and http://www.nfpa.org. The NFPA is an international nonprofit codes and standards organization. NFPA 1600 is a description of the basic criteria for a comprehensive program that addresses disaster recovery, emergency management, and business continuity.

P1.3.3 Physical Security (PS)

PS1: The provider controls physical access to information assets and IT services and resources based on their importance, and monitors and reviews all physical access. This includes

a. identification and authentication of client and provider staff members who have physical access to assets providing client services
b. the process for requesting and approving physical access
c. whether the physical assets are dedicated to the client or shared by multiple clients
d. how physical assets are physically and securely segregated from other provider assets and other client assets
e. client asset protection from unauthorized physical access

PS2: The provider demonstrates the presence of physical security systems such as uninterruptible power supplies, backup generators, redundant climate control systems, and a data-center-grade fire control system for prevention and protection.

P1.3.4 Data Handling (DH)

DH1: The provider handles client data in accordance with the data's classification (e.g., confidential, sensitive, public) and complies with client data handling requirements (policies, procedures, regulations). (The client provides these requirements.) Media is visibly marked to identify the data's classification. The provider describes how access to highly confidential client data is protected and controlled. Provider staff members that require access to such data are identified and trained in the access requirements for this data. [BITS 01, Section 5.4.1, p 28]

DH2: The provider protects highly confidential and sensitive data by using defined chains of custody and removable storage media, creating backups that are stored off site, using encryption for data creation, transfer, and storage where required, and having a discard process for such data and its storage media. Refer also to P1.3.9 Backups. [BITS 01, Section 6.2, 6.5, p 38, 39]

DH3: All client and provider programs, data, and written materials are protected from unauthorized copy, use, duplication, and storage. [BITS 01, Section 5.4.9, p 28]

DH4: The provider describes retention guidelines for various classes of data (such as user data, backups, logs, monitoring results, and reports) based on client requirements. Such guidelines specify how long data is retained online, its storage format and archive process, and how long the archives are available for data retrieval.

DH5: The provider prevents inadvertent disclosure of client data by ensuring proper erasure of media used to store intermediate and final client files before this media is reused. [BITS 01, Section 5.3.3, p 27]

P1.3.5 Authentication and Authorization (AA)

AA1: The provider has implemented appropriate levels of user authentication and control of user access. User access can occur through network connections from both inside and outside the provider's organization.

Provider practices are consistent with security policies and procedures. Provider practices take into account levels of restricted access required for specific assets and levels of data classification.

AA2: The provider requires the use of at least two-factor authentication for administrative control of all network infrastructure devices to include switches, gateways, routers, firewalls, VPNs, and network segment monitoring systems such as intrusion detection systems.

AA3: The provider protects critical assets when authenticating and authorizing users and administrators working remotely (as well as third parties such as tiered service providers). This is implemented by using strong encryption and virtual private networks, access controls at the level of networks, systems, files, and applications, and by restricting access to authorized times and tasks as required. These practices apply to wireless network access as well.

AA4: The provider uses mechanisms such as digital signatures for ensuring non-repudiation where it is critical to validate the sender's or originator's identity.

AA5: For systems at the client's site, the client has the responsibility to ensure that the provider cannot access non-service systems. The provider should also take steps to ensure that provider staff members are not permitted onto other client systems. This may involve setting access permissions for specific provider user groups on service systems residing at the client's site. The client can then specifically block these groups on non-service systems, either by user group name or network address. The same precautions should be taken for systems located at the provider's site.

P1.3.6 Access Control (AC)

AC1: The provider affirms that only duly authorized staff members who use and support requested service systems have access to the operating system, applications, and databases to be used in providing the requested services. Access controls

a. apply to provider and client staff members
b. specify which uses of the system are authorized and how all others are denied/prohibited (such as unacceptable hardware and software installations)
c. establish access request, access review, and access termination processes
d. are consistent with client policies and procedures. (These are provided by the client.)

AC2: The provider's access controls include processes for access request, access review, and access termination.

AC3: The provider's process for requesting new or changed access to service assets includes [BITS 01, Section 6.1.1, p 37]

a. a process definition or flow
b. access levels for development and support of service assets
c. approval authority for access ID requests (provider, client, both)
d. responsibility for implementation and maintenance of access IDs (provider, client, both)
e. validation of access ID authorizing signatures

AC4: The provider's process for reviewing new or changed access to service assets includes [BITS 01, Section 6.1.2, p 37-38]
   a. responsibility for creation and maintenance of access authorization lists
   b. responsibility for review and approval of access authorization lists
   c. review frequency of access authorization lists
   d. a process to ensure timely change or deletion of access upon employee transfer and/or termination
   e. a process for timely validation of access request changes, accomplished through reviewing the changes made in comparison to the changes requested

AC5: The provider has implemented a range of security controls to protect client and provider assets residing on service systems and networks to include
   a. access controls at the level of networks, systems, files, and applications
   b. data encryption (including key protection/distribution) and virtual private network technologies. In cases where strong encryption is required to protect asset confidentiality, the provider uses tested, proven encryption algorithms (such as AES, 3DES[10], and RC4[11]) and keys longer than 40 bits.
   c. an approach to cryptographic key management including PKI (Public Key Infrastructure) details such as certificate authorities, directory server management, key recovery, and the use of PKI applications. [Cisco 01] Client and provider should review key management periodically to ensure that there are no weaknesses in the cryptosystem. (Refer to Practice 5.)
   d. perimeter and internal firewalls that implement security policy
   e. removable storage media for critical data so that it can be physically secured
   f. a system discard process that eradicates all data from disks and memory prior to disposal.
   g. means for client data, system, network, and performance protection from exposure to other clients when the service executes on shared servers or devices

AC6: The provider's SOC operates on a local network, which is accessible only by operations staff who are physically inside the center. Physical SOC access is restricted to authorized staff members.

P1.3.7 Software Integrity (SI)

SI1: The provider verifies the integrity of installed software by
   a. regularly checking for all viruses, worms, Trojan horses, and other malicious software and eradicating them
   b. keeping up-to-date virus signatures and other relevant signatures such as those for intrusion detection systems
   c. regularly comparing all file and directory cryptographic checksums with a trusted baseline
   d. regularly verifying that client data stored on provider equipment is appropriately segregated from the data of other clients [BITS 01, Section 6.2, p 38]

---

[10] Advanced Encryption Standard and Triple Data Encryption Standard. See http://csrc.nist.gov/cryptval/des.htm.

[11] RC4 is a stream cipher designed by Rivest. See http://www.rsasecurity.com/rsalabs/faq/3-6-3.html.

Verifying software integrity includes verifying software written by the client (or expressly for them) and used by the provider [BITS 01, Section 5.6.6, p 30].

P1.3.8 Secure Asset Configuration (SC)

The provider has deployed and documented procedures and processes to ensure the secure configuration of all client information assets throughout their life cycle (installation, operation, maintenance, retirement). These are described below.

SC1: The provider requires authentication on both ends of the communication when changes to the configuration are requested. This may include rotating passwords or pass phrases to verify user authenticity, and also their authorization to make changes.

SC2: The provider applies patches to correct security and functionality problems. What is the documented schedule for patching the software on service systems? Is there a scheduled time period to patch systems (i.e., a time period on a specific day of the week where routine, non-critical patches are applied to service systems)? How does the patching schedule affect service availability requirements? How quickly does the provider implement patches that address known vulnerabilities?

SC3: The provider establishes a standard, minimum essential configuration for each type of computer and each type of service, storing this as a trusted base configuration. Actions to be taken include removing or disabling all unnecessary applications and services (producing a minimum essential configuration), removing default accounts, and patching known vulnerabilities. Does the provider have a process for securely configuring service systems prior to deployment, and for keeping the system's security configuration up to date? Are configurations tested in a non-production environment prior to deployment? These questions apply to service systems at both provider and client sites.

SC4: The provider enables adequate levels of logging to validate the asset's security status.

SC5: The provider has well-established, documented configuration management and change control procedures as well as test procedures that are exercised when changes are made. This includes the ability to recover from upgrade and patch installation problems, backing out all relevant changes and establishing a previously working configuration. This also includes client approval of pending changes, if warranted, and client notification when changes are made that can affect client service processing, performance, and data.

SC6: The provider tests all service system configurations after installation. How is this performed and how often? As configuration changes are made, the provider needs to test the configuration to ensure it is still working as intended. Testing may include scanning and probing, as well as vulnerability assessment and penetration testing of the system. These types of tests reveal whether the current configuration is operating as intended. These results should be reported to the client on a regular basis.

SC7: The provider considers the security implications for all changes to provider systems and networks.

SC8: The provider performs vulnerability assessments and penetration tests on a regular basis and addresses weaknesses in a timely manner when they are identified.

Describe how frequently assessments are performed, how the provider stays abreast of the latest vulnerabilities[12], what tools are used, and how the most critical weaknesses to address are identified (versus the thousands that some tools report). See also P1.1.4 Independent Evaluations and Practice 8.

SC9: The provider asserts that no undocumented, unreported configuration changes will occur.

P1.3.9 Backups (BU)

BU1: The provider specifies a regular schedule of backups for both software and data that includes

a. how often backups of certain types (partial, full) are performed
b. validating software and data before backup
c. validating software and data after backup
d. verifying the ability to restore from backups including being able to accommodate client requests for unscheduled backup restoration
e. the capability to back up critical data more frequently. (The client identifies such data.)
f. identifying how long backup media is retained and if this can be specified by the client
g. isolating this client's backup media from that of other clients
h. the use of encryption

BU2: The provider describes how they perform backups of service system configuration files. The description answers the following questions:

a. How are these files stored?
b. Are they encrypted? Are they digitally signed?
c. Who has access to them?
d. Are they stored off-site?
e. Is there a well-defined chain of custody process as backup media moves from location to location?

It is advisable to sign and encrypt these files, as they can contain sensitive information about the service infrastructure. It is also prudent to severely restrict user access to these files. Providers should keep configuration files for a reasonable amount of time, usually one year, in the event that they are compromised or failures occur, requiring an archived, known, trusted copy of the configuration files to be reinstalled.

P1.3.10 Monitoring and Auditing (MA)

This practice describes actions the provider takes to monitor and audit its own systems and networks. It also applies to client systems and networks if the requested services include monitoring and auditing. For further details, refer to Practice 7.

[12] Four excellent information sources about current vulnerabilities and patches are the CERT Coordination Center at http://www.cert.org, SANS at http://www.sans.org, Common Vulnerabilities and Exposures at http://www.cve.mitre.org/, and Bugtraq at http://www.bugtraq.com.

MA1: The provider uses appropriate monitoring, auditing, and inspection facilities and assigns responsibility for reporting, evaluating, and responding to system and network events and conditions. This includes

a. regularly using system and network monitoring tools and examining the results they produce
b. regularly using log filtering and analysis tools and examining the results they produce
c. filtering raw logging information using automated tools to decrease the amount of information that analysts need to review

The provider describes how often monitoring results are reviewed as part of normal operations.

MA2: The provider asserts that monitoring results and log files are generated in a write once-read many (WORM) mode so that they cannot be overwritten or tampered with, and that they are stored on read-only media. This guarantees that unauthorized users cannot alter or delete file contents.

MA3: The provider describes

a. how often monitoring is performed and whether or not this is done in real time
b. how systems and networks are monitored
c. if monitoring includes all network traffic entering and leaving the network
d. if monitoring includes the entire network (firewalls, intrusion detection systems, routers, servers, niche security products, customer applications) and how correlation from all data sources is performed
e. how significant monitoring results are reported
f. how monitoring results are stored, including logs
g. how monitoring tools are protected and ensured to be secure

MA4: The provider describes their ongoing processes for global vulnerability and threat analysis as well as the sources used for such analysis.

P1.3.11 Incident Management (IM)

The provider describes the following processes for both client and provider systems involved in executing requested services.

IM1: Incident reporting and triage. This process involves the provider reviewing reports of suspicious system and network behavior and events (an incident). Such reports often result from monitoring and auditing. A sound incident reporting and triage process ensures that all staff members know whom to contact when they notice suspicious behavior and that they know how to take user reports into account. The process includes

a. performing "triage" upon receipt of a report, making an initial assessment about its severity
b. evaluating, correlating, and prioritizing each report
c. investigating each report or set of related reports
d. determining that an attack or intrusion has occurred and initiating the intrusion detection process

IM2: Intrusion detection: This process includes alert handling, describing what actions and countermeasures are taken when alerts are generated. For example, all alerts are handled initially by automation, and when human action is required, a notification process delivers the information to an analyst. Include how this process is adapted to address new threats.

IM3: Intrusion response: This process includes

a. handoff from intrusion detection
b. triage of all detected intrusions and how triage priorities are established
c. how the service responds to a detected intrusion including
    1. internal provider supervisor/manager notification. Describe escalation decision points and timing. For example, notification could occur within one and a half hours of detection to the first level supervisor, four hours to the next level up, eight hours to the next level, and sixteen hours to the responsible executive/senior manager. Times are likely to vary based on the negotiated service level.
    2. notifying the client (describe escalation decision points and timing)
    3. containing the damage
    4. returning systems to normal operation
    5. exercising options for automated response
    6. performing forensic analysis
    7. preserving evidence
    8. involving local, national, and international law enforcement [Cisco 01]
    9. recommending improvement actions to ensure the same intrusion is not successful again

IM4: The provider describes the following process review approaches:

a. how the client is informed and involved in these processes (IM1, IM2, IM3), including client roles, responsibilities, and approval authority.
b. how often and under what conditions intrusion detection and response processes are exercised and tested. Include a summary of the scenarios and test cases that are used to conduct such testing. The best of provider organizations practice their responses to security incidents by performing exercises. This approach results in their being better prepared when a real event happens, and they then respond with skills that have been honed through practice sessions and exercises.

IM5: The provider confirms that these processes are documented and available to the client, if such documentation is not included in the proposal.

P1.4 Case Studies

This section gives the provider an opportunity to describe how their services have performed in an operational setting. The response is intended to provide scenario-based information that a client can use to evaluate the presence or absence of business attributes, service attributes, and security practices. Some of this information can be verified through independent sources.

Service Scenarios
Describe the top three to five service-based events or incidents that the provider was involved in during the last twelve months. Describe the service delivery flow including automated support as well as staff analysis and support and client involvement. For example, during and after an attack on a client's systems and networks, describe the provider's role in managing attack detection and response.

If providers are unwilling to describe specific scenarios due to client confidentiality requirements, consider posing several hypothetical scenarios that are meaningful to the client organization and ask the provider how they would address them.

Market Position
Describe why you would buy your service instead of contracting with one of your top three competitors. Identify what distinguishes your services in the marketplace as well as areas for improvement and future development.

P1.5 Checklist

Consider making a checklist modeled after Table 1 to support your RFP preparation. It may be necessary to add sub-entries under each attribute and practice to create a complete checklist. Consider including some form of the proposal evaluation matrix shown in Practice 2, section P2.4 in the RFP as a means by which to amplify the client's priorities and requirements and, perhaps, ensure more responsive proposals.

Table 1: MSS RFP Checklist

RFP Requirement	Include	Exclude	Tailor
P1.1 Provider Business Attributes			
P1.1.1 Viability (VI)			
P1.1.2 Client Satisfaction (CS)			
P1.1.3 Relationships with Other Parties (RO)			
P1.1.4 Independent Evaluations (IE)			
P1.1.5 Personnel (PR)			
P1.1.6 Asset Ownership (AO)			
P1.1.7 Contractual Exception, Penalties, and Rewards (CE)			
P1.1.8 Service Level Agreement (SA)			
P1.1.9 Exit Strategy (ES)			
P1.1.10 Site Visit (SV)			
P1.1.11 Implementation Plan (IP)			
P1.1.12 Points of Contact (PC)			
P1.2 Provider Service Attributes			
P1.2.1 Top-level Security Requirements (SR)			
P1.2.2 Service Availability (SY)			
P1.2.3 Service Architecture (ST)			
P1.2.4 Service Hardware and Software (HS)			
P1.2.5 Service Scalability (SS)			
P1.2.6 Service Levels (SL)			
P1.2.7 Reporting Requirements (RR)			
P1.2.8 Service Scope (SP)			
P1.2.9 Cost (CO)			
P1.3 Provider Security Practices at Provider Site			
P1.3.1 Security Policies, Procedures, and Regulations (PP)			
P1.3.2 Contingency Planning; Operational and Disaster Recovery (DR)			
P1.3.3 Physical Security (PS)			
P1.3.4 Data Handling (DH)			
P1.3.5 Authentication and Authorization (AA)			
P1.3.6 Access Control (AC)			
P1.3.7 Software Integrity (SI)			
P1.3.8 Secure Asset Configuration (SC)			
P1.3.9 Backups (BU)			
P1.3.10 Monitoring and Auditing (MA)			
P1.3.11 Incident Management (IM)			

P1.3 Provider Security Practices at Client Site			
P1.3.1 Security Policies, Procedures, and Regulations (PP)			
P1.3.2 Contingency Planning; Operational and Disaster Recovery (DR)			
P1.3.3 Physical Security (PS)			
P1.3.4 Data Handling (DH)			
P1.3.5 Authentication and Authorization (AA)			
P1.3.6 Access Control (AC)			
P1.3.7 Software Integrity (SI)			
P1.3.8 Secure Asset Configuration (SC)			
P1.3.9 Backups (BU)			
P1.3.10 Monitoring and Auditing (MA)			
P1.3.11 Incident Management (IM)			
P1.4 Case Studies			
Service Scenarios			
Market Position			

Practice 2: Guidance for Evaluating an MSS Proposal

This practice contains guidelines for evaluating the merits of MSS proposals that have been submitted in response to a client-developed RFP for managed security services. To be acceptable, the provider's proposal must demonstrate how they intend to meet the requirements described in the RFP. This includes specified business attributes (P1.1), service attributes (P1.2), and security practices (P1.3). The purpose of evaluation is to verify that the provider has a well-developed approach to providing requested security services. The evaluation will also show whether or not the provider has adequate resources and the business experience needed to ensure a high quality, continuous level of service. [BITS 01, Section 4, p 19]

Along with a review of all RFP requirements and the guidelines outlined in this practice, the client's proposal evaluation should include [BITS 01, Section 4, p 19]

- a review of the provider's strategy, reputation, experience, and financial condition
- a list of any tiered providers that the provider relies on to deliver service, how client requirements flow to tiered providers, and how tiered providers are held accountable for meeting client requirements
- a consideration of the cost of switching providers if the selected provider fails to meet contractual requirements. For example, what are the cost implications if the provider's solution is proprietary?
- a list identifying any user groups associated with the service and the provider's practice of communicating with clients through such groups
- an assessment of the level of client trust in the provider as well as their responsiveness and quality-of-service (used to make a decision about service renewal) [Pescatore 02]

When evaluating each provider's proposal, keep the next step in mind: developing a contract and a service level agreement. In particular, consider those cases where the provider's proposal response may require modification, where the provider's standard SLA may require modification or augmentation, and where the provider's standard operating procedures may not be acceptable to the client.

We recommend that a client verify proposal contents and claims by

- requiring an evaluation by a trusted third party or results from a recently performed review (if the third party conducting the review is acceptable to the client)
- performing reference checks based on referrals provided by the provider and sought independently
- conducting site visits where the service will be performed

Providers can find it burdensome to respond to the wide range of potential business opportunities including requests for proposals, all of which have unique requirements. Clients should consider using recent provider certifications, evaluations, and other credible sources that accurately represent the provider's condition. If the provider can use one general set of results to respond to several business opportunities, this aids both client and provider in maintaining a reasonable cost of doing business.

When evaluating a provider's proposal, a client needs to understand the level of risk in outsourcing any managed security service (see Introduction) to ensure that the cost to procure, operate, and manage provider service delivery and ensure service level agreement (SLA) compliance do not exceed the anticipated benefit.

P2.1 Business Attributes

Business attributes are one element of client requirements. They comprise characteristics, policies, processes, and procedures that need to be described in a qualified RFP response and include

- Viability (VI)
- Client Satisfaction (CS)
- Relationship with Other Parties (RO)
- Independent Evaluations (IE)
- Personnel (PR)
- Asset Ownership (AO)
- Contractual Exceptions, Penalties, and Rewards (CE)
- Service Level Agreement (SA)
- Exit Strategy (ES)
- Site Visit (SV)
- Implementation Plan (IP)
- Points of Contact (PC)

The provider's proposed solution must satisfactorily address and comply with all business attributes presented in the client's RFP. Guidelines for evaluating specific provider business attributes are presented below.

P2.1.1 Viability (VI)

Viability guidelines are organized in six categories. These are

- VI1: Financial
- VI2: Services Offered
- VI3: Organizational Breadth
- VI4: Investment Strategies
- VI5: References

VI1: Financial

a. Annual revenue or investment funding information give a good indication of a provider's financial status. For publicly traded companies, annual revenue of more than $10M per year in MSS contracts indicates a sufficient base of revenue to support growth and enhancement of services. If possible, select a large, publicly traded company that has the ability to weather temporary downturns in the economy [Navarro 01]. For privately funded startups, funding of more than $25M provides adequate cash reserves. At least 75 percent of a provider's personnel should be involved in revenue-generating efforts: sales, SOC operation, and services delivery [Pescatore 01b].
b. The mix of provider personnel is close to 50:50 between operational SOC employees and billable consultants. An equal mix of operational SOC personnel and billable consultants result in subscription services generating between 70 and 85 percent of revenue [Pescatore 01a].
c. The provider carries adequate levels of insurance. The provider can withstand service claims against them or a catastrophic incident and remain financially viable.
d. Broad name recognition (or "mindshare" to use a currently popular term) is an indication of the provider's marketing and communications campaign. The provider is perceived as a leader in the marketplace, demonstrated by press exposure, proactive detection and promulgation of security vulnerability alerts, effective seminar and education programs, and a good reputation according to peer providers and clients.
e. Consider providers with at least three years of experience [Radcliff 00].

VI2: Services Offered

a. The provider offers a comprehensive range of services and has the flexibility to meet a broad range of security needs. The provider has technical depth, expertise, and a mix of technical skills (managed services, audits, penetration testing, architecture, implementation assistance) to provide services reliably [Armstrong 01]. However, avoid providers that have conflicts of interest. For example, some providers offer security management and monitoring. If the provider finds a security problem with a client's network, will the provider tell the client or try to fix it quietly? Providers that both sell and manage security products have the same conflict. If a client outsources security device management, it is essential that it outsource its monitoring to a different provider [Schneier 02].

VI3: Organizational Breadth

a. Breadth in the type of channel partners (resellers) indicates a provider's ability to increase and support its client base without having to build out an expensive direct sales channel and to spread its costs. Marketplace leaders are likely to acquire more than 40 percent of their clients from channel partners across multiple regions and all segments of the security services and product markets [Pescatore 01b]. Providers that do not expand beyond regional clients will not be long-term survivors [Pescatore 01a].

b. Be aware of special relationships the MSSP has with tiered providers. Evaluate the extent to which such relationships have influenced provider product and service recommendations. Be sure these are the right recommendations to satisfy client requirements.

VI4: Investment Strategies

a. Successful providers need liquidity for business development, research and development, and infrastructure maintenance. A successful provider will have at least 10 percent of its personnel allocated to research and development or be aligned with a SOC provider that does so [Pescatore 01a]. Also look at the provider's installed base and the percent of clients who have multi-year contracts [Pescatore 01b].
b. The provider demonstrates a record of investment and innovation in security practices [Armstrong 01].

VI5: References

a. When conducting a provider client reference check, ask the following questions: [CIO 01]
    1. Is the client still using the service? If not, why not?
    2. What services is the client using? What is their configuration, version, and what are their features? Make sure that the client is using a service comparable to the one you are evaluating. If the client has experienced service version upgrades, ask if the transition to the new version was easy or difficult.
    3. How is the client using the service?
    4. How did the client choose the provider? What are the strengths and limitations of the provider's service?
    5. What are some of the problems the client has experienced with the provider and with the service? How has the provider handled these? Have they all been successfully resolved? If not, how are disputes handled?
    6. How long did it take to transition to the new service? What were the key issues?
    7. How is the provider's customer service?
    8. Is there a provider service user's group? Does the client attend? If not, why not?
b. Consider performing background checks and financial viability checks for smaller provider firms [Radcliff 00].
c. Consult other credible, reputable sources of information to establish the viability of the provider's organization such as
    1. Dun & Bradstreet and other credit agency reports
    2. analysts of advisory firms such as Gartner, Giga, etc.
    3. analysts at securities firms
    4. the provider's competitors and industry opinion leaders to learn what's being said about the provider in the marketplace
    5. current and past provider clients other than those offered as a reference by the provider

d. If the managed security services can be competently delivered by a provider with whom you have an existing, trusted relationship, seriously consider this provider first [Radcliff 00].

P2.1.2 Client Satisfaction (CS)

CS1: Confirm responsiveness, hours of staff availability, and available communication mechanisms (e.g., written, verbal, electronic, face-to-face, secure) with other provider clients who have used similar services.

The Hurwitz Group, a technology research and consulting firm, states that "The best way to understand a vendor's commitment to its customers is to examine its service and support practices and policies. Understanding a vendor's service philosophy provides a view into what the ongoing experience with the vendor will be like. Companies need to be sure that the vendor has practices and procedures in place to proactively support customers, and to provide them with information or fixes quickly, sometimes even before the customer may know they need the fix." They provide the following checklist for purchased software, all of which can be applied to managed security services [Hurwitz 02]:

Do look for

- around-the-clock (24x7) availability, in multiple languages
- multiple communication methods such as web, email, and self-service, not just by telephone
- a provider-sponsored community of practice (more than just a user's group)
- bulletin boards, chat rooms, and download sites
- opt in subscriptions to problem/fix announcements
- support for procedural questions outside of consulting engagements
- timely problem resolution
- published support targets with a high attainment level

Watch out for

- restricted support hours or languages
- different response standards for telephone inquiries versus those entered via the web
- procedural and educational issues always resulting in a consulting engagement
- unhappy or nonexistent user groups
- attempts by the provider to keep users apart
- no procedure for proactively notifying clients of problems
- lack of published performance targets, goals, and attainment results

P2.1.3 Relationships with Other Parties (RO)

RO1: Evaluate the provider's reliance on tiered (third party) providers to provide the requested service(s). [BITS 01, Section 4, p 19]

a. Identify and review all provider dependencies.
b. Verify the process the provider has in place to review tiered providers' security policies and procedures.

c. Review the provider's service record and experience with tiered providers.
d. Review the provider's issue notification, communication, and contingency plans for tiered providers.
e. Evaluate interoperability security between the provider and any tiered providers.
f. Evaluate the extent to which written permission from the client is required for a tiered provider to access and use client data.

RO2: Evaluate the types of contractual arrangements in place to assure that both the provider and its critical tiered providers (e.g., the SOC provider) have long-term commitments to each other to minimize the chance of abandoning the client [Pescatore 01a].

RO3: Evaluate what impact the provider will have on other provider relationships that already exist in the client's operational environment [BITS 01, Section 4.3, p 21].
a. Review access control, security, and privacy requirements from previously established provider relationships to evaluate whether any of them are affected by the new relationship.
b. Review network configurations to assess whether logical or physical separations are required between provider connections and access points.
c. Review existing provider contract terms to evaluate whether any are affected by the new provider relationship.
d. Review existing insurance terms and conditions to evaluate whether any are affected by the new provider relationship.

RO4: Does the provider have relationships with ISPs to handle upstream reporting of attacks or probes and scans? When there are issues to be reported and coordinated, choosing a provider that has close ties to upstream providers is a benefit. A provider's close relationship to an ISP will make it easier to deal with and control scans, probes, and denial-of-service attacks carried out against provider and client systems. Larger providers have close relationships with the large ISPs and use their relationships as leverage to help the client deal with such problems.

P2.1.4 Independent Evaluations (IE)

IE1: Determine if the provider and their tiered providers have one or more evaluation reports that can be used to demonstrate satisfaction of RFP requirements. Are the reports from the current-year? Were the evaluations independently conducted? Reports need to address testing of general and technology-based requirements (attributes and practices) for services specified in the RFP and at the site where services will be performed.

In the event that the third-party evaluation report does not address the scope or location of the services being processed, the client should retain the right to evaluate the facility, the operational environment, implementation of certain policies, and adherence to client-specific policies, procedures, and practices [BITS 01, Section 4.1, p 20]. Based upon the level of risk associated with the services to be performed, the client may require an additional review of the provider's hardware, software, processes, and practices. [BITS 01, Section 4.1, p 19]

IE2: The client should verify that applicable service requirements are satisfied based on actual test results. The client should determine if the report is for the current year, if there have been any changes to the infrastructure or configuration of the systems and networks since the last review or test, and whether the location and operational environment associated with the tested services are materially the same. If so, these service components should undergo a further review to ensure that the provider has maintained integrity. It is critical that the client verify that the reviewed systems and infrastructure are the same as those that will be hosting the requested services. [BITS 01, Section 4.1, p 20]

IE3: A thorough provider security review includes testing the operational services environment (i.e., where the requested services will be installed and performed). A range of audit, assessment, evaluation, and penetration test approaches are available. However, depending on the service to be outsourced, the cost of such a review may be prohibitive. It is important to understand the level of risk involved in using the outsourced service and whether it operates within a shared or dedicated processing environment. For a business-critical service that handles sensitive data, a thorough test should be conducted. As the level of risk decreases, alternative approaches may be considered. They may include any subset of the guidelines included below, as well as system scans, vulnerability research and identification, and references from other clients. [BITS 01, Section 4.1, p 19]

IE4: The types of tests should require written sign-off by the client and the provider because of the potential for service disruption, financial loss, and the triggering of certain automatic security responses. Tests and test results should include [BITS 01, Section 4.1, p 21]

a. security policies and procedures
b. physical security
c. external network penetration attempts
d. internal penetration attempts
e. vulnerability assessments
f. attempts to gain access through social engineering techniques
g. a complete report of attacks and tools used, findings, and recommendations
h. a follow-up review to confirm that recommendations were implemented
i. a determination of whether testing was performed for each service attribute and security practice

IE5: If the provider performs internal evaluations, the client may want to evaluate the process used to conduct these reviews and the results produced.

IE6: The selection and use of independent evaluators should be mutually acceptable. A written agreement between all parties grants evaluation permission and specifies that the evaluator may not disclose any of the proprietary information of the provider or client. Give the provider advance notice and details of the review's scope to minimize any impacts to availability, service levels, client satisfaction, etc. Share results with the provider within a specific time frame after an evaluation is performed. Discuss and mutually determine items that may need resolution and/or develop plans and procedures to address any changes suggested by the evaluation. [BITS 01, Section 4.1, p 20]

P2.1.5 Personnel (PR)

PR1: The provider should have expertise and significant current business in the client's vertical market. [Radcliff 00]

PR2: Successful providers are those that demonstrate mastery in the business issues of providing quality MSS rather than those with solely the most in-depth security expertise [Pescatore 01a]. Successful providers have skills and depth in many areas outside of information and network security [Pescatore 02].

PR3: Management experience in this type of service is evident and includes facility development and management, brand development and marketing, device monitoring, software development, and managing service line margins. Look for past experience in service bureaus, outsourcers, online services, and financial services [Pescatore 01b].

PR4: Watch out for providers that have lots of technical knowledge but little understanding of methodologies or business practices [Radcliff 00].

PR5: A provider can allocate service support staff on a round robin basis by alert (like a help desk) or can dedicate staff to a specific client (the latter option is preferable). A dedicated analyst can provide better advice about the ongoing management of all security services for a particular client.

PR6: "Properly staffing a SOC seat around-the-clock requires six full-time security management engineers. This is required to cover all hours in the day including vacation, sick leave, training, etc." [ISS 01] Ensure the provider has adequate and qualified staff to cover SOC operations around-the-clock and year-round (24x7x365).

PR7: Evaluate the provider staff need-to-know and the appropriate level of authority they need to have in order to access client data [Alner 01]:

a. Identify the people who are required to sign confidentiality agreements, the staff roles they hold, and the purpose of the agreements.
b. Identify the requirements for provider staff bonding and under what conditions bonding is required.
c. Identify the provider staff members who require privileged access and the rationale for this access

PR8: Ensure that the provider's due diligence with respect to personnel policies and procedures meets client requirements.

P2.1.6 Asset Ownership (AO)

AO1: The provider identifies assets that will be used in providing client services and who owns them. Assets include networks, systems, software, hardware, source code, processes, concepts, policies, reports, logs, evaluation results, other data, and the like. This includes assets existing prior to the contractual relationship and assets acquired and created during the contract's performance. The provider identifies which data belongs to the client and which data requiring client access belongs to the provider. This is important because the data owner determines the access rights.

As an example, the ownership of policies and procedures can become an issue. If the provider writes policies and procedures for the client but owns the copyright, the client cannot change them without approval from the provider. [Alner 01]

AO2: The provider describes how assets will be transitioned at the end of the contract where ownership is retained by the provider but where ongoing client use is required. This includes such assets as software licenses obtained by the provider on the client's behalf.

P2.1.7 Contractual Exception, Penalties, and Rewards (CE)

CE1: Evaluate the provider's standard contract language and clauses to make sure they are both sufficient to meet client requirements, including requirements mandated by regulatory and legislative bodies. (Refer also to P1.3.1 Security Policies and Regulations.) If the language or the contract clauses are not sufficient to meet client requirements, then address the deficiencies and choose remedies during the negotiation of the contract. Refer to Practice 3 for further details.

P2.1.8 Service Level Agreement (SA)

SA1: The provider offers well-defined SLAs with clear measurement criteria and financial penalties for non-performance [Armstrong 01].

SA2: Ensure that the provider's SLA addresses client requirements and that the process for its modification allows for new or tailored client-specific requirements to be included.

P2.1.9 Exit Strategy (ES)

ES1: Evaluate the provider's standard contract language and clauses to make sure those addressing contract termination are sufficient to meet client requirements. If not, address deficiencies and remedies during contract negotiation. Refer to Practices 3 and 6 for further details.

P2.1.10 Site Visit (SV)

SV1: "Visit the provider's SOC and take your best security/technical person with you. Don't just do a physical walkthrough – ask to have your security person sit next to their specialists and see the technology and process. If the vendor tells you they keep visitors 'behind the glass' for security reasons, there may be something they aren't comfortable sharing." [James 02].

SV2: Develop a site visit checklist to include all applicable business attributes, service attributes, and security practices that can be reviewed and demonstrated in accordance with the provider's proposal. Identify and communicate any additional requirements or demonstration scenarios that are not called for in the RFP that you intend to examine.

P2.1.11 Implementation Plan (IP)

IP1: Evaluate the provider's implementation plan to make sure it meets client requirements. Refer to Practice 4 for further details.

P2.1.12 Points of Contact (PC)

PC1: The provider identifies points of contact who will serve as the primary interface between the two organizations for proposal evaluation and service level agreement (SLA) preparation and negotiation. These points of contact may not be the people responsible for managing the day-to-day client/provider interface once the contract is signed.

P2.2 Service Attributes

Service attributes are a second element of client requirements. They describe the quality of service to be provided and levels of service performance to be met and include

- Top-level Security Requirements (SR)
- Service Availability (SY)
- Service Architecture (ST)
- Service Hardware and Software (HS)
- Service Scalability (SS)
- Service Levels (SL)
- Reporting Requirements (RR)
- Service Scope (SP)
- Cost (CO)

To qualify, a proposal must demonstrate how the provider will ensure compliance with all service attributes during the execution of the contract, as presented in the client's RFP. The client needs to evaluate the provider's proposal to make sure it meets client requirements (refer to P1.2 Service Attributes). Guidelines for evaluating specific provider service attributes are presented below.

P2.2.1 Top-level Security Requirements

Refer to P1.2.1.

P2.2.2 Service Availability (SY)

SY1: Ensure that provider staff coverage and expertise match service availability requirements.

SY2: Evaluate service availability features and the role each feature plays in satisfying overall service availability requirements [BITS 01, Section 4.4, p 21].

SY3: Ensure that the service outage time caused by the provider is calculated from the moment of client impact until the service is fully restored with no initial outage time exclusions [Nicolett 02].

Review the following outage conditions and evaluate whether or not they are acceptable [BITS 01, Sections 4.4.1-4.4.3, p 21-22]:

a. regularly scheduled time periods when the service is not available
b. how scheduled service software and hardware maintenance affect service availability

SY4: Understand how additional service volume created by a new client affects both client and provider system performance and availability, and if this is acceptable. [BITS 01, Sections 4.4.1-4.4.3, p 21-22]

SY5: Review the provider's historical statistics about system availability and response times for the requested service and evaluate their acceptability. They can be used as a predictor of future performance.

P2.2.3 Service Architecture (ST)

ST1: Evaluate the provider's architectural features for high availability and operational redundancy. [BITS 01, Section 4.4.4, p 22]

ST2: The provider adequately demonstrates that clients do not compromise each other's processing environment or data. If provider computers such as servers and storage devices are shared with multiple clients, the provider demonstrates how they ensure that no client can access another's data, systems, and networks. [Alner 01]

ST3: Evaluate how the provider's service solution integrates with the client's in-house security devices and technologies. It is highly desirable to achieve ROI on currently implemented service approaches to the greatest extent possible. [Armstrong 01]

ST4: "Pay attention to how the provider manages network connectivity, bandwidth, carrier relations, and device health. If the provider cannot show best practice-based policies and procedures for its own systems, you cannot be certain that those systems will be able to serve your company." [ISS 01]

P2.2.4 Service Hardware and Software (HS)

HS1: Verify that the provider's service hardware and software solutions are compatible with the client's operational environment.

HS2: The provider augments off-the-shelf monitoring tools with in-house technology for security management and monitoring. Both are needed since no commercial solution available today can handle the demands of monitoring thousands of security devices from a wide range of providers [Pescatore 01a].

HS3: Review and understand the provider's process for maintenance of service hardware and software, including how often maintenance is performed for provider site and client site assets and how the provider reports the outcomes of maintenance activities.

P2.2.5 Service Scalability (SS)

SS1: Evaluate the ability of the provider's service architecture to provide and support growth in the client's capacity requirements [BITS 01, Section 4.4.5, p 22].

P2.2.6 Service Levels (SL)
Refer to P1.2.6.

P2.2.7 Reporting Requirements (RR)
Refer to P1.2.7.

P2.2.8 Service Scope (SP)

SP1: To lower initial risk and learn how to best work with a new provider, consider implementing the smallest, most well-defined, least intrusive service/service feature first, gradually adding in more service capability over time. Look for providers that allow such incremental changes in client service coverage. [DeJesus 01]

P2.2.9 Cost (CO)

CO1: Cost depends heavily on contracted services, service levels, bandwidth, the number of computers being monitored, and the like. Simple monitoring and notification is usually least expensive, since it is largely automated. Analysis costs more, depending on the level. Response costs more still, since that almost always involves human decisions and actions.

CO2: Economies of scale allow providers to be cost-competitive. If a provider is monitoring 10,000 networks, adding one more is not going to require a major upgrade in resources. Monthly fees as low as $1,000 are not unusual; at the higher end, expect to pay the equivalent of one salaried IT professional.

CO3: Most providers charge a monthly or yearly subscription fee that provides a specific level of service. The fee often depends on how many servers the provider is protecting, the quality of service, and the speed. There may be additional fees for a provider's initial analysis of a client's security posture and for any non-routine customization.

CO4: Ensure that the provider's proposed solution does not cost more than the value of the client assets being protected.

P2.3 Security Practices

Security practices are a third element of client requirements. The provider's proposal must demonstrate that their services meet or exceed the client's security policies and procedures and that all security practices are effectively implemented and in use, as specified in the RFP. This includes demonstrating that

- the provider's network and system infrastructure is well secured, as well as that of any tiered providers to whom they subcontract
- the client's network and system infrastructure remain well secured when the provider's service is deployed

Keep in mind that specific practice implementations vary depending on the provider's operational environment and the service being provided. Guidelines for evaluating specific provider security practices are presented below.

Practice topics include

- Security Policies, Procedures, and Regulations (PP)
- Contingency Planning; Operational and Disaster Recovery (DR)
- Physical Security (PS)
- Data Handling (DH)
- Authentication and Authorization (AA)
- Access Control (AC)
- Software Integrity (SI)
- Secure Asset Configuration (SC)
- Backups (BU)
- Monitoring and Auditing (MA)
- Incident Management (IM)

P2.3.1 Security Policies, Procedures, and Regulations (PP)

PP1: Evaluate the provider's non-compliance with security policies specified by the client as well as any conflicts between the client's and provider's (and any tiered provider's) security policies, procedures, and regulations. If issues arise, ensure they can be resolved in the SLA. [Alner 01]

PP2: Verify that provider policies and procedures are enforced and that consequences for non-compliance are clearly stated.

P2.3.2 Contingency Planning; Operational and Disaster Recovery (DR)

DR1: Evaluate the recovery time objective for the provider to restore systems. Also determine the average time delay between system restoration and service availability. Determine that times have been demonstrated in testing and that they are acceptable. [BITS 01, Section 4.7, p 22]

DR2: Evaluate if the provider has established "preferred priority restoration" with other clients of their services. [BITS 01, Section 4.8, p 23]

a. Determine if other clients have contracted for recovery priority.
b. Determine the estimated restoration window for the system with preferred priority restoration and without this priority.
c. Determine the probability of other clients declaring a disaster simultaneously.
d. Evaluate the contingency plans in place to support multiple clients' recovery events.

DR3: Evaluate the provider's capabilities for notifying you of a service outage including [BITS 01, Section 4.9, p 23]

a. the provider's procedures for notifying the client in the event of planned and unplanned outages.
b. procedures and timeframes for problem reporting and escalation, for both the provider and the client.

Refer also to P1.2.2 Service Availability and P1.2.7 Reporting Requirements.

DR4: Review the provider's reliance on tiered providers to provide a recovery environment. Evaluate [BITS 01, Section 4.10, p 23]

a. if the tiered providers are capable recovery service providers
b. if the provider has had to declare a disaster requiring the activation and use of a tiered provider's resources, and how well the effort succeeded
c. certifications and capabilities of provider's tiered providers including having physical security at least comparable to the security of the provider's operational site [Alner 01]
d. if the provider can leverage the client's existing relationship(s) with other tiered providers
e. the conditions under which a tiered provider site would be activated
f. the level of access required for a tiered provider site

DR5: Review the provider's documented recovery procedures for both individual systems used in day-to-day service and a full site outage. [BITS 01, Section 4.11, p 23]

a. Evaluate the differences between operational and disaster recovery.
b. Evaluate the suitability of the provider's disaster recovery site as a client DR site in the event of a local disaster.

DR6: Review recent recovery testing efforts, including the scope and results of the test. [BITS 01, Section 4.12, p 23-24]

a. Evaluate if the requested services have been tested successfully and how frequently services are tested.
b. Evaluate the scope of tests including depth (such as operating system, service software, service databases, network) and breadth (such as operational, disaster).
c. Determine if testing is certified by an independent third party and, if so, review the certification.
d. Determine if there have been significant upgrades or other changes to relevant systems since the last time they were tested that would require retesting.
e. Verify that the client can choose to be involved in testing the disaster recovery plan on a regular basis [Alner 01].

DR7: Evaluate if the provider supports a dual, high-availability environment in the event of a natural disaster and interruptions in local/regional utility service (for example, communications, gas, electric, sewer, water). If the provider is located in an earthquake zone, flood plain, or hurricane/tornado area, evaluate risk mitigation approaches in the service site's physical construction and operation. [BITS 01, Section 4.4, p 22]

DR8: If tiered provider sites (or elements of the provider's organization/site delivering service) are located outside of the client's primary country of operation, evaluate how readily services can be transferred from international sites to secondary recovery sites, both within and outside of the provider site's country.

DR9: Consider integrating the provider's BC/DR plan into the client's own business continuity plan. [BITS 01, Section 4.5, p 22]

a. Verify that emergency response procedures are in place to help ensure timely relocation of key personnel.
b. Verify that client service relocation procedures support proper client notification and status support.
c. Verify that the plan is updated as needs change. [Alner 01]

P2.3.3 Physical Security (PS)

PS1: Confirm by a site visit that physical security requirements are satisfied and physical security practices are being followed.

P2.3.4 Data Handling (DH)

Refer to P1.3.4.

P2.3.5 Authentication and Authorization (AA)

Refer to P1.3.5.

P2.3.6 Access Control (AC)

Refer to P1.3.6.

P2.3.7 Software Integrity (SI)

Refer to P1.3.7.

P2.3.8 Secure Asset Configuration (SC)

Refer to P1.3.8.

P2.3.9 Backups (BU)

Refer to P1.3.9.

P2.3.10 Monitoring and Auditing (MA)

Refer to P1.3.10.

P2.3.11 Incident Management (IM)

Refer to P1.3.11.

P2.4 Evaluation Matrix

Consider making an evaluation matrix (as shown in Table 2) to support the evaluation of the proposal. Construct it using the same entries as the RFP checklist described in Section P1.5. You may need to add sub-entries under each attribute or practice to create a complete matrix.

Include some form of this evaluation matrix in the RFP to help convey the client's priorities and requirements. This should help ensure more responsive proposals.

Table 2: MSS Proposal Evaluation Matrix

RFP Requirement	Relative Weight (scale of 1-10)	Points Awarded	Meets Reqmts. (yes/no)	Comments
P2.1 Provider Business Attributes				
P2.1.1 Viability (VI)				
P2.1.2 Client Satisfaction (CS)				
P2.1.3 Relationships with Other Parties (RO)				
P2.1.4 Independent Evaluations (IE)				
P2.1.5 Personnel (PR)				
P2.1.6 Asset Ownership (AO)				
P2.1.7 Contractual Exception, Penalties, and Rewards (CE)				
P2.1.8 Service Level Agreement (SA)				
P2.1.9 Exit Strategy (ES)				
P2.1.10 Site Visit (SV)				
P2.1.11 Implementation Plan (IP)				
P2.1.12 Points of Contact (PC)				
P2.2 Provider Service Attributes				
P2.2.1 Top-level Security Requirements (SR)				
P2.2.2 Service Availability (SY)				
P2.2.3 Service Architecture (ST)				
P2.2.4 Service Hardware and Software (HS)				
P2.2.5 Service Scalability (SS)				
P2.2.6 Service Levels (SL)				
P2.2.7 Reporting Requirements (RR)				
P2.2.8 Service Scope (SP)				
P2.2.9 Cost (CO)				
P2.3 Provider Security Practices At Provider Site				
P2.3.1 Security Policies, Procedures, and Regulations (PP)				
P2.3.2 Contingency Planning; Operational and Disaster Recovery (DR)				
P2.3.3 Physical Security (PS)				
P2.3.4 Data Handling (DH)				

P2.3.5 Authentication and Authorization (AA)				
P2.3.6 Access Control (AC)				
P2.3.7 Software Integrity (SI)				
P2.3.8 Secure Asset Configuration (SC)				
P2.3.9 Backups (BU)				
P2.3.10 Monitoring and Auditing (MA)				
P2.3.11 Incident Management (IM)				
P2.3 Provider Security Practices At Client Site				
P2.3.1 Security Policies, Procedures, and Regulations (PP)				
P2.3.2 Contingency Planning; Operational and Disaster Recovery (DR)				
P2.3.3 Physical Security (PS)				
P2.3.4 Data Handling (DH)				
P2.3.5 Authentication and Authorization (AA)				
P2.3.6 Access Control (AC)				
P2.3.7 Software Integrity (SI)				
P2.3.8 Secure Asset Configuration (SC)				
P2.3.9 Backups (BU)				
P2.3.10 Monitoring and Auditing (MA)				
P2.3.11 Incident Management (IM)				
P2.4 Case Studies				
Service Scenarios				
Market Position				

Practice 3: Content Guidance for an MSS Service Level Agreement

The SLA contains "...contractually binding clauses documenting the performance standard and service quality agreed to by the client and the provider. The SLA's primary purpose is to specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met." [BITS 01, Appendix 4, p 62]

In effect, the SLA is an agreement between the client and the provider quantifying the minimum acceptable service from the client's perspective [Hiles 02]. The SLA is probably the most important document in a MSS client/provider relationship. An SLA, when properly written, is distinguished by clear, simple language and a focus on the needs and wants of the client's business [CIO 01]. Creating a sound, mutually agreeable SLA is a matter of due diligence by both parties.

A provider typically has developed an SLA that they are comfortable with, based on service level measurement averages across a range of clients. Providers want clients to accept their SLA as the contractual agreement. "All too often, provider service-level agreements have the facade of service assurance, but in reality, they are designed to limit the liability of the provider. Providers that construct SLAs to protect their revenue stream commonly use a combination of nonspecific or unmeasurable service indicators[13], exclusions that negate what appear to be rigorous service commitments, and penalties that are capped at a small percentage of the provider's revenue." [Nicolett 02]

"An SLA is a binding contract which specifies the provisioning of performance and service quality parameters between two legal entities (the provider and the client). Don't simply sign off on a service provider draft. Engage a lawyer familiar with commercial law as well as new economy law (including intellectual property), and have the lawyer co-develop the SLA with your service provider and their legal counsel." [NM 01]

Clients should go into the negotiation process with their own SLA as the starting point, taking the provider's proposal into account. The client's SLA should be aligned with their own critical assets, protection strategies, policies and procedures, and should be defined to satisfy confidentiality, integrity, and availability requirements.

Clients need to determine the most critical aspects of a service and then ensure that SLAs are defined and negotiated to address them. These are likely to include service security, service levels, service response times, infrastructure uptime/downtime, network performance, scalability, reporting, client and client customer satisfaction, overall end-to-end performance of service features, and escalation processes.

[13] For example, "Many SLAs specify service-level calculations that are based on broad averages of site availability. Service-level measurements that are based on broad averages tend to mask the measurement of limited, but damaging, outages of a small number of critical applications." [Nicolett 02]

The SLA defines the roles of both the client and the provider. As a result, the client understands exactly what they are expected to do and what the provider is agreeing to do on the client's behalf. The SLA should be as precise as possible. It needs to define what client resources the provider will be accessing and what functions the provider may perform on these resources [Navarro 01]. It is critical to involve all client stakeholders who will be responsible for ensuring SLA compliance in the SLA development process. This includes IT and security staff members.

"Where several suppliers are involved in the end-to-end delivery of a service, back-to-back SLAs are necessary so the lead supplier can provide an end-to-end SLA to the customer. These back-to-back SLAs may also be known as tiered SLAs or multi-tiered SLAs." [Hiles 02]

To the extent contractually possible, all guidelines described below should be applied to all tiered providers involved in delivering service. Where this is not possible, the provider must describe to the client how the tiered provider will be held accountable for all service level agreement requirements in which they participate. Clients should consider inserting a contract or SLA clause stating that the primary provider remains accountable for any damages or sub-par performance caused by tiered providers.

The overall contract between client and provider includes the SLA. In addition to covering SLA contents, this practice provides guidance on other security-related contract content that is typically outside the scope of the SLA. At a minimum, an SLA defines service specific performance measures (primarily described in P3.3). Some of the guidelines contained in P3.2 Business Attributes are appropriate for an SLA and some may be more appropriate for other sections of a client/provider contract. Similarly, P3.4 Security Practices describes the quality of operational security practice expected from the provider when they are the custodian of the client's information assets, regardless of the specific service. Again, some of these guidelines may be more appropriate for other sections of a client/provider contract. Regardless, for this practice, all requirements are described as being part of a service level agreement. It remains for the client and provider to determine how best to present this information in a contractual form.

A note on terminology: The literature uses the term "SLA" to connote the overall agreement/contract on service level scope, function, and performance as well as individual, detailed measurements for each service requirement. In this practice, we use the former definition. Individual measurements are referred to as service levels, service level measurements, or service agreements, and do not use the SLA acronym.

P3.1 General SLA Guidelines

A Service Level Agreement should contain the following sections:

1. Executive Summary:
   This is an overview and description of the document's purpose, which is generally to perform the services described and meet or exceed individual service agreements that have been negotiated. The summary includes the agreement's duration and identifies the client's key stakeholders and owners responsible for managing each service and ensuring service agreements are met.
2. Service(s) Description:
   This section contains a detailed description of services and the negotiated service agreements associated with each. There is one subsection for each category of service (for example, firewall management, intrusion detection system management, remote access, and vulnerability assessment). There are additional subsections for business attributes or security practices that are service-independent or span multiple services.

   Service Level Definitions:

   For each service, key service descriptors should be included as follows:

   a. Definition: A precise, unambiguous description of the service that is being performed, measured, and reported.[14]
   b. Measurement time frame: Points in time (days, dates, and times) when service measurements are to be made. Indicate if the scope includes all 365 days of the year or if selected days are excluded. Describe the timeframe (typically days or weeks) over which measurements are to be made such that the client can then determine if the service agreement is exceeded, met, or not met.
   c. Responsibilities: Specific roles and responsibilities of client and provider that need to be fulfilled to comply with service agreements. Identify who is responsible for making each measurement and how each measurement is validated. Identify primary and secondary points of contact for both organizations as well as all tiered providers.
   d. Service level metrics:
      1) Measurements and measurement ranges for the contracted service such as service availability or response times.[15] Typically, service levels are described as percentages. However, providers need to propose measurements stated in client business performance terms, with client assistance.

[14] For example, "To provide a comprehensive managed security solution that allows remote employees and business partners to connect to the internal network and data resources using an IP-VPN." [NM 01]
[15] For example, "In an SLA for Internet access, you may list the acceptable range for availability as between 99.9 to 99.999 per cent. If you are buying technical support services, you may list the acceptable range for response time as between four to six hours after a support call is initiated." [NM 01]

2) Watch for service level metrics that are calculated based on the aggregate performance of multiple assets (such as multiple servers). Average performance across multiple assets will rarely fall below agreed-upon levels even if critical assets are not performing acceptably. Make sure that service level metrics for critical assets are individually identified.
3) Where a service level range is acceptable, consider specifying a desired service level as well as a minimum acceptable (worst case) level, with rewards and penalties tied to each.
4) For service levels that are difficult to determine in advance without some supporting operational experience, consider a specified timeframe of pilot implementation and review before they are documented in an SLA.

e. Measurement formula: This describes the mathematical measurement equation to be used and an example. Identify any performance monitoring/measurement tools used by the provider and document client confirmation that these tools are acceptable.
f. Shared services: When multiple clients share provider service resources, overconsumption by one client may affect the performance of another. This can be addressed with a provider guarantee of adequate capacity, implementation of blocking when demand exceeds established limits, or by the option to purchase exclusive access to the service.
g. Data sources: This describes where measurement data is collected, what is collected, where it is collected, how it is stored, and who is responsible for collecting it.
h. Escalation activity: When out-of-compliance situations occur, describe who is notified and under what conditions. This includes day-to-day and measurement period situations that are out of compliance, as well as system outages, site outages, and other relevant business continuity and operational/disaster recovery situations.
i. Contractual exceptions, rewards, and penalties: This describes all negotiated exceptions, rewards[16], and penalties[17] that are included in the SLA and apply to this service. Indicate client and provider reporting responsibilities for noting an exception, a reward, or a penalty.

[16] For example, "If the service provider over-delivers for one year with no major incident, you may automatically extend an additional year upon the lapse of the contract with no need for a new contract." [NM 01] "Incentives should not be paid for exceeding SLAs unless they can provide true business value. If a vendor introduced a plan for an innovation that improves service and the plan contains a business case that shows savings, it may be appropriate to share half of the first year's cost savings with the vendor." [Nicolett 02]

[17] "It is not reasonable to expect [a provider] to agree to 'total cost of downtime' penalties, but there should be enough loss of revenue potential in the SLA to provide an incentive to the provider. Providers that are confident in their ability to execute will offer SLAs with accelerating rebate penalties and high penalty caps." [Nicolett 02]

Some providers require client notification in writing, within a given timeframe, to receive penalty payments or credits.[18] See also P3.2.7.

j. Reward/penalty formula: This describes the mathematical equation to be used and an example. If the client or provider uses severity or priority codes, these are also described in this section.

3. Service Level Management:

Document the following processes necessary for managing service levels. Include the event or timeframe that triggers process execution:

a. measurement tracking and reporting
b. problem escalation and dispute resolution
c. service change requests including renegotiating service measurement terms. Make sure to specify that service levels are periodically reviewed and updated to match industry standards [CIO 01].
d. implementing new services and service levels
e. service level review process
f. approval process

4. Roles and Responsibilities:

The section describes general or over-arching roles and responsibilities of all parties that are not covered under Service Level Definitions above. This includes the client, the provider, any tiered providers, and any governance committees or key stakeholders managing this contract.

As part of their responsibilities, clients should provide

- complete and thorough details of the client's infrastructure architecture and network environment where provider services are to reside
- timely, complete information about necessary client changes and problems such as network configuration upgrades, problems with Internet connectivity, major discovered vulnerabilities, and unusual network activity

5. Appendices:

Appendices include more detailed information that may be relevant. For example, an appendix could discuss provider-supported hardware, software, and chargeback procedures.

As part of the SLA creation process, the client ensures and affirms that other SLAs with this same provider do not conflict with the SLA under negotiation [Alner 01].

[18] For example, Verio's SLA states "Verio will issue a credit to Customer for Outages occurring during any calendar month, provided such Outages (i) in the aggregate, exceed ninety (90) minutes, (ii) are reported by Customer to Verio, (iii) either (A) are confirmed in the Customer's monthly IS Services reports as provided on Customer's IS Services Control Panel, or (B) in the event that Verio's measurement equipment is inoperable or faulty, can be reasonably demonstrated by Customer to have occurred using industry standard measurement tools." This SLA later states "In order to receive a credit under this SLA, a request therefore must be made by Customer in writing via the Customer's IS Services Control Panel." [Verio]

P3.2 Business Attributes

Business attributes are one element of client requirements. They comprise characteristics, policies, processes, and procedures that need to be precisely defined and mutually agreed to in the SLAs and the client/provider contract. They include

- Viability (VI)
- Client Satisfaction (CS)
- Relationship with Other Parties (RO)
- Independent Evaluations (IE)
- Personnel (PR)
- Asset Ownership (AO)
- Contractual Exceptions, Penalties, and Rewards (CE)
- Service Level Agreement (SA)
- Exit Strategy (ES)
- Site Visit (SV)
- Implementation Plan (IP)
- Points of Contact (PC)

The Service Level Agreement must satisfactorily address all business attributes presented in the client's RFP as modified by the provider's proposal. Guidelines for describing provider business attributes are presented below.

P3.2.1 Viability (VI)

VI1: Consider incorporating provisions for client notification in the event of [BITS 01, Section 5.2, p 26; Section 5.13.3, p 34]

a. impending cessation of the provider's business or that of a tiered provider and any contingency plans in the event of notice of such a failure (refer to Practice 6)
b. financial difficulty that may impact service delivery
c. significant changes in tactical or strategic decisions regarding the purchase and support of hardware or software related to service processing
d. significant staffing reductions or changes in key staff that may affect the provider's ability to deliver the agreed-upon support and service
e. a decision to outsource, sell, or acquire significant operations or support associated with the applications, data, network, or other critical component of the environment used to provide client services. See Relationships with Other Parties in this section.
f. pending press releases on any subject that may impact the client

VI2: Consider incorporating provisions for client asset protection in the event of one or more of the above notifications:

a. Grant the client's right to access and wipe/degauss their systems, disk drives, backup tapes/disks, and the like to prevent sensitive data from staying on equipment scheduled to be sold.
b. Tag client equipment to establish client ownership and maintain an up-to-date, validated hardware inventory to prevent client equipment from being seized and sold. This also resolves questions of ownership in the event the provider's business is acquired.

P3.2.2 Client Satisfaction (CS)

CS1: Describe the level of client service support to be provided including hours of service, use of automated methods, problem resolution times, and guaranteed time for call-back [BITS 01, Section 5.1.1, p 25].

CS2: Consider having the provider (and tiered providers) agree to periodically conduct a client satisfaction survey and report the results to the client. The survey is intended to qualitatively measure the client's perception of service quality. Survey results can be factored into provider service reward/penalty formulas (refer to P3.1 General SLA Guidelines and service attribute descriptions below). Include factors such as [Hiles 02]

a. service availability and response time
b. ease of use
c. quality of customer service support
d. training
e. acceptable downtime including cost or impact

In the absence of provider agreement, the client may want to consider conducting such a survey internally and reporting the results to the provider.

P3.2.3 Relationships with Other Parties (RO)

RO1: The client and provider execute any required documents that grant written permission for a tiered provider to have access to and use client data.

RO2: The provider documents support responsibilities and hours of operation for all tiered providers involved in delivering contracted service.

RO3: The provider asserts that they are contractually responsible for tiered provider performance including the satisfaction of all service agreements in which the tiered provider participates.

RO4: The provider demonstrates the means they use for communicating service agreements to tiered providers and for ensuring that tiered providers meet these agreements.

P3.2.4 Independent Evaluations (IE)

IE1: The provider regularly provides the client with the results from full systems audits, security risk evaluations, vulnerability assessments, and penetration tests performed by a mutually agreeable third party [Alner 01]. The SLA specifies who performs each evaluation and how often this is to be done. The contract between the client and the provider defines what events or circumstances trigger these evaluations as well as who incurs the cost. The client may consider requiring that the client's internal audit staff be given, at a minimum, annual access to perform operational, information technology, and/or financial audits of the provider.

IE2: The client and provider discuss items that may need to be resolved and then mutually set priorities and resolution plans [BITS 01, Section 4.1, p 20]. The client may want to specify timeframes for certain classes of items requiring resolution such as high-priority vulnerabilities identified through a vulnerability assessment.

P3.2.5 Personnel (PR)

PR1: The client should explicitly identify skills transfer as a key objective of the relationship with the provider to ensure the client can knowledgeably manage the service and in the event the client's eventual goal is to bring the service in-house [Cramm 01].

PR2: The client and provider execute written confidentiality and non-disclosure agreements, where required.

PR3: The provider needs to ensure that client staff members are not inadvertently creating security exposures as a result of ignorance. This can be addressed by conducting awareness and training programs and by monitoring users' actions [Alner 01].

P3.2.6 Asset Ownership (AO)

AO1: The SLA or contract

a. describes how assets will be transitioned at the end of the contract where ownership is retained by the provider but where ongoing client use is required. This includes such assets as software licenses obtained by the provider on the client's behalf.
b. should transfer necessary data intellectual property rights and copyrights from the provider to the client so the client can update data items in the future and use them at the end of the contracted relationship. [Alner 01]

Refer to P2.1, Asset Ownership and Practice 6 for additional details.

P3.2.7 Contractual Exceptions, Penalties, and Rewards (CE)

CE1: The SLA specifies courses of action that can be taken if the agreements are not met (on either side). Consider bonuses for service delivery above stated standards or non-monetary rewards such as documenting the client's experience as a public-relations case study. Negotiate penalties for substandard service, including restitution. The client needs to understand the liability associated with security breaches by either party, including the limitation of damages. Document legal implications if either party fails to fulfill its obligations. [Alner 01]

CE2: A reputable provider should be willing to absorb a penalty of up to 100 percent of its charges in a given reporting period as compensation for service level failures.[19] If the provider is not prepared to accept this, they should be treated with considerable caution [Hiles 02]. Watch for provider-proposed penalty caps such as twelve to eighteen months of service fees and any clauses stating that any specific performance penalty is the sole and exclusive remedy of the customer [CIO 01].

[19] Some examples of service level penalties for a web site hosting service include: (1) one day of free service for each 15 minutes of downtime, with a maximum of one month free each month, (2) one free day if the service is down for 26 seconds, and (3) one free day for each five (accumulated, not consecutive) minutes of downtime [Turek 00]. Another provider offers a "service credit" worth one day of service, but no more than seven credits can be accumulated in a one-month reporting period.

CE3: The SLA should specify that service levels can be renegotiated during contract performance. This description should specify any predetermined conditions under which such negotiation might occur.

P3.2.8 Service Level Agreement (SA)

Refer to P1.1.8, P2.1.8, and P3.1.

P3.2.9 Exit Strategy (ES)

ES1: Make sure that the contract includes a description of what constitutes normal contract completion as well as earlier than anticipated termination. Termination can occur under the following circumstances: termination for cause including breach of contract such as inability to perform or serious breaches of security (confidentiality, integrity, availability)

a. convenience
b. provider insolvency or bankruptcy
c. change of provider business ownership or control such as that which occurs during mergers and acquisitions

See also P3.2.1 Viability for other events that trigger client notification and possible contract termination conditions that need to be considered.

ES2: Ensure this description addresses

a. outgoing provider responsibilities including those necessary to ensure a smooth transition of service with minimal disruption to the client
b. client responsibilities
c. transfer of key assets (data, software, hardware, tools). Where the provider retains ownership for service application source software, the contract includes the following details:
    1. a third party escrow location, agreed to by both parties, where the baseline version of the software will be held
    2. contractual requirements to maintain currency and completeness of the source code (and associated documentation)
    3. determination of who pays the escrow costs, as well as specific conditions under which the escrow is available to the client
    4. designated client and provider points of contact 1) who provide access to materials for verification, 2) in the event any of the clauses are invoked, such that the client gets the source code, to whom the source code is released, and when it will be released
    5. the type of media on which the source code is stored
    6. specification of all elements of the operational environment under which the source code is readable/executable, etc.
d. destruction and/or return of client proprietary and other sensitive information
e. penalties levied by the provider and damages paid to the client should any current or past provider staff member violate terms of a non-disclosure agreement or any other agreement that extends beyond the contract's period of performance
f. transition timeframe

For further details, refer to Practice 6.

P3.2.10 Site Visit (SV)

Refer to P1.1.11 and P2.1.11.

P3.2.11 Implementation Plan (IP)

Refer to P1.1.12, P2.1.12, and Practice 4.

P3.2.12 Points of Contact (PC)

PC1: Identify the client and provider points of contact that will serve as the primary interfaces between the two organizations for service implementation and day-to-day management.

P3.3 Service Attributes

Service attributes are a second element of client requirements. They describe the quality of service to be provided and levels of service performance to be met and include

- Top-level Security Requirements (SR)
- Service Availability (SY)
- Service Architecture (ST)
- Service Hardware and Software (HS)
- Service Scalability (SS)
- Service Levels (SL)
- Reporting Requirements (RR)
- Service Scope (SP)
- Cost (CO)

In an SLA, the provider describes how they will demonstrate compliance with all service attributes during the execution of the contract, as presented in the client's RFP and as modified by the provider's proposal. Service attributes include service levels and performance standards, the client's responsibility in support of them, reporting requirements, responsibilities for troubleshooting, problem escalation, continuous improvement provisions, and the consequences and remedies of non-performance [BITS 01, Section 5.1.2, p 26]. Guidelines for specific provider service attributes are presented below.

P3.3.1 Top-level Security Requirements (SR)
Refer to P1.2.1.

P3.3.2 Service Availability (SY)

SY1: Describe the process and timeframe for service implementation.

SY2: Describe service availability timeframes and any limitations, up to twenty-four hours a day, seven days a week, and 365 days a year, depending on the service.

SY3: Describe service uptime using the RFP guidelines.

SY4: Specify response time when a service outage occurs and services are not available. Guaranteed Response Time (GRT) is a key SLA requirement. Specify provider response time guidelines to address client requirements on service systems that the provider is managing such as response time

a. to discover attempted or successful intrusions
b. to implement configuration change requests
c. to deploy a patch against a new vulnerability
d. following service hardware and software maintenance

SY5: The provider collects sufficient information to report downtime for the reporting period, reasons for any outages, and service level impacts of any outages.

SY6: Describe anticipated efficiencies to be gained from improvements in technology [BITS 01, Section 5.1.2, p 26].

P3.3.3 Service Architecture (SA)

Refer to P1.2.3 and P2.2.3.

P3.3.4 Service Hardware and Software (HS)

HS1: Describe the software and hardware support services to be provided [BITS 01, Section 5.1.1, p 25].

P3.3.5 Service Scalability (SS)

SS1: The provider collects and reports capacity-related statistics such as bandwidth utilization and percent of service system capacity used. The client specifies anticipated rates of client capacity growth, storage needs, and seasonal or promotional spikes [BITS 01, Section 5.1.2, p 26]. The provider projects any anticipated impact caused by capacity growth on service availability and performance standards.

P3.3.6 Service Levels (SL)

SL1: Define and describe specific service performance requirements such as response times (speed of notification attempts), service processing times, frequency of monitoring, time to problem resolution, and supporting analysis activities [BITS 01, Section 5.1.2, p 26].

SL2: Consider the use of a balanced scorecard that summarizes and prioritizes service levels by weighting them based on their relative importance. In cases where a provider meets or exceed service levels, positive "points" are awarded. Performance below service levels results in points being subtracted. If the total points score is below an agreed-upon threshold, the client can invoke penalties [Hiles 02].

SL3: Specify how emergencies will be handled. Identify whose authorization is required to fix problems, which problems will be handled by the client, and which will be handled by the provider.

SL4: Specify how special client requests are handled, including additional costs and turn-around time. [Alner 01]

P3.3.7 Reporting Requirements (RR)

RR1: For each type of report, specify the frequency, format, and content. Attach sample reports to the SLA. Include

a. service level measurements reports such as the provider service performance as measured against minimum service levels
b. violations reports: actual or attempted user logon violations and access violations
c. incident reports: actual or attempted intrusions

RR2: Negotiate report content that is based on the actual end-user experience with a service, rather than an aggregate of system response metrics. These types of reports provide a more meaningful representation of what the end user is experiencing.

RR3: Specify the maximum timeframe for posting new problems and action items into the problem tracking system following their discovery. This may be based on an agreed-upon description of problem criticality, with the most critical problems being posted in the shortest possible timeframe (hours).

P3.3.8 Service Scope (SP)

SP1: Describe the client's right to make changes to services and the required process and obligations to add new services, modify current services, or combine multiple services [BITS 01, Section 5.1.1, p 25-26].

SP2: Describe "emerging technology considerations and provisions for replacing, reducing or adding services based upon technology changes" [BITS 01, Section 5.1.1 p 26].

P3.3.9 Cost (CO)

Not applicable; addressed outside of the SLA.

P3.4 Security Practices

Security practices are a third element of client requirements. The provider's service performance must comply with the client's security policies and procedures. The provider demonstrates that their security practices are effectively implemented and in use, as specified in the RFP and as modified by the provider's proposal. This includes demonstrating that

- the provider's network and system infrastructure is well secured, as are those of any tiered providers to whom they subcontract
- the client's network and system infrastructure remain well secured when the provider's service is deployed

The SLA should address details of RFP-specified security practice topics including

- Security Policies, Procedures, and Regulations (PP)
- Contingency Planning; Operational and Disaster Recovery (DR)
- Physical Security (PS)
- Data Handling (DH)
- Authentication and Authorization (AA)
- Access Control (AC)
- Software Integrity (SI)
- Secure Asset Configuration (SC)
- Backups (BU)
- Monitoring and Auditing (MA)
- Incident Management (IM)

Specific SLA considerations for some practices are described below.

P3.4.1 Security Policies, Procedures, and Regulations (PP)

PP1: The client needs to determine what requirements are fully or partially implemented by the provider's services. Such requirements include regulatory, legislative, standards, policy, and other requirements. The client explicitly allocates those requirements where the provider is involved to the provider. The provider needs to accept this allocation. Both client and provider need to ensure that this sharing of responsibility can satisfy a third party evaluation of these requirements, demonstrating successful provider compliance.

PP2: Check for conflicts between client and provider security policies and procedures. If conflicts exist, resolve them in the SLA.

PP3: Both client and provider can demonstrate that they are exercising an appropriate standard of due care with respect to securing information assets. This is primarily accomplished through security policies and procedures that are documented and enforced, and security practices that are deployed. [Alner 01]

PP4: The provider describes the mechanism used to verify user compliance with the provider's password policy as well as any other user authentication procedure

PP5: The provider demonstrates that their implementation of separation of duties is consistent with the client's requirements, including: (1) security administration, review of user access, and incident reporting, and (2) between provider development, operations, and consulting staff. Address other potentially conflicting roles, as necessary. [BITS 01, Section 5.6.5, p 30]

P3.4.2 Contingency Planning; Operational and Disaster Recovery (DR)

DR1: The provider describes situations requiring operational recovery, recovery time objectives (how long it takes to recover), recovery point objectives (how far back—to what point in service processing—to recover, considering what information may have been lost).

DR2: In the event of a disaster or similar emergency, the provider specifies the minimum and maximum

a. recovery timeframes associated with provider and client computing assets
b. time for client data validation
c. time that the client will be without provider services

DR3: Determine the provider's problem escalation policies, processes, and reporting timeframes. Timeframes for escalation reporting must match the client's requirements. For serious security issues, a short reporting timeframe is appropriate (15 minutes is the standard). For less critical issues, a timeframe of one hour, one day, or "in the monthly report" may be acceptable. The client needs to designate what constitutes categories such as serious, less critical, and so on.

P3.4.3 Physical Security

Refer to P1.3.3 and P2.3.3.

P3.4.4 Data Handling (DH)

DH1: The provider's use of client data for data mining or any purpose other than the service processing directly contracted for by the client is not permitted without the express written permission of the authorized client data owner.

DH2: The provider affirms that all client data will be removed from all computers and media that is upgraded, deployed, and retired.

P3.4.5 Authentication and Authorization (AA)

AA1: The provider states a response time range for

a. providing new user access from the time of receiving the request [BITS 01, Section 5.5.1, p 29]
b. creating, changing, or deleting a user ID or password

AA2: The provider retains a record of all authorization and access requests including the originator of the request. [BITS 01, Section 5.5.2-5.5.3, p 29]

P3.4.6 Access Control (AC)

AC1: Determine which data belongs to the client and which data requiring client access belongs to the provider. The data owner determines the access rights.

AC2: Document requirements for the use of encryption, the maintenance of keys, and any related infrastructure requirements. Address "the entire end-to-end transaction (e.g., origination, storage, network path, backups, recovery, and any legally mandated provisions)." [BITS 01, Section 5.4.7, p 28]

AC3: The SLA should specify (1) what assets the provider must be able to access to perform the contracted service, and (2) that the client is willing and able to grant such access. [DeJesus 01]

P3.4.7 Software Integrity (SI)

SI1: Specify the frequency with which the provider compares key asset cryptographic checksums with the trusted, securely stored baseline set of checksums. Specify the events that cause the baseline to be updated.

P3.4.8 Secure Asset Configuration (SC)

SC1: The provider informs the client of any hardware or software changes that could affect them, before they are made. These types of changes could involve anything from installing a new server to upgrading the security software. If required, the client should be given the opportunity to test these changes before they are deployed and provide feedback to the provider. [Alner 01]

SC2: All provider changes that could affect client service or data along with anticipated client impact are communicated to the client designated point of contact. The client may need to negotiate retaining the right of approval on all such changes. This service level specifies the number of days or weeks of advance notification to the client.

SC3: For vulnerability assessments and penetration tests, identify client and provider roles and responsibilities, assessment frequency, timeframe for notification of identified vulnerabilities, and, based on vulnerability risk level, resolution timeframe. Such testing should be coordinated with the provider and it should not result in system availability issues, missed service levels, downtime, or client dissatisfaction. [BITS 01, Section 5.7, p 31]

SC4: The provider specifies the process and timeframe for patch application and verification.

SC5: Specify that undocumented, unreported configuration changes are cause for contract penalties. The client can identify these by performing a configuration review, a vulnerability assessment including penetration testing, and by a successful intrusion that takes advantage of an undocumented change.

P3.4.9 Backups (BU)

BU1: Define responsibility for data backup. Include

- guidelines for backup frequency (such as weekly for full backups and daily for partial backups)
- time for restoration from backups
- retention timeframe (such as one month of backed up files at the primary site)
- destruction timeframe
- offsite storage location and timeframe (such as one year of backed up files at the secondary/disaster recovery site)

In addition, the provider needs to describe guidelines for full life cycle data protection (creation, use, destruction).

BU2: If provider is managing service systems that are critical to the client's mission, then system downtime can affect a client's ability to fulfill it. Consider an agreement specifying an acceptable timeframe to restore data from a trusted backup after equipment failures or other system problems.

BU3: Specify a penalty level for failing to succeed in performing backups successfully within the required timeframe.

P3.4.10 Monitoring and Auditing (MA)

Refer to P1.3.10.

P3.4.11 Incident Management (IM)

IM1: Describe the level of incident events that the provider handles (assuming the provider is performing ongoing monitoring) and what level of event gets turned over to the client [Alner 01]. This includes whether or not the client will be consulted before any action takes place. Some providers prefer to act first to stop the attack and then inform the client what happened. [DeJesus 01]

IM2: Specify provider roles and responsibilities in the event of an attack. A provider's response can vary widely from post-attack notification to on-the-spot consultation to full responsibility for real-time response, investigation, and civil or criminal proceedings. Any limitation in the provider's response puts an additional burden on the client. Specify key contact personnel (including backups) in both organizations, how they are to be notified, and under what conditions. [DeJesus 01]

IM3: If the provider is to handle client user/client customer security problems and questions, SLA guidelines should delineate what the provider should handle, whose authorization is required to address routine problems, and what types of issues should be referred to the client's own staff. [Alner 01]

IM4: Describe the required data for violation reports and the provider's availability to support any investigation. The review and investigation of these violations may be best handled by the client's own staff because they are more likely to know which data is critical. [Alner 01]

IM5: The client and provider need to agree on the requirements and process for handling incidents and then document them, assuming this service is provided. See also P1.3.11 Incident Management.

This process includes [BITS 01, Section 5.6, p 29-30]

a. identifying what constitutes an incident and its level of severity
    1. actual or attempted user logon violations and access violations
    2. penetration attempts on provider systems and networks used to perform client services
    3. penetration attempts on client systems and networks
b. logging all incidents
c. escalation and follow-up monitoring including circumstances under which the service is shut down
d. automated notification (e.g., via alerts) of serious incidents and to whom
e. logs (in a secure electronic format) being provided to the responsible party for review; how long such logs are retained
f. the time lag between the incident and verbally notifying the client
g. any requirement for redundant notification based upon the severity of the incident (such as telephone, email, fax, and/or pager)
h. restoration time for data that is lost or damaged
i. forensics analysis
j. civil or criminal investigation including interfacing with law enforcement

IM6: The client or provider may be faced with assuming "the costs of remediation for security issues where this is due to failure to fulfill obligations prior to the breach or other violation." [BITS 01, Section 5.6, p 29] As a result, it is critical that roles and responsibilities be clearly defined in the abovementioned incident handling process.

Practice 4: Transitioning to MSS

Initiating a managed security services relationship may require a complex transition of people, processes, hardware, software, and other assets from the client to the provider. IT and business environments may require new interfaces, approaches, and expectations for service delivery. Roles and responsibilities are often redefined. [Ambrose 01]

This practice describes steps to effectively move from the execution of the MSS contract to full production use of the provider's managed services. We refer to this as the implementation phase. This phase "can be the most challenging and the highest-risk period in the lifecycle of an outsourcing relationship. An implementation that is not well planned and managed may result in overall failure, client inconvenience and dissatisfaction, or unexpected operational support costs [BITS 01, Section 7, p 40]." The absence of a comprehensive, mutual plan is a high risk. In long-term, outsourced relationships, the key people who are initially involved in developing the relationship, negotiating the contract, and developing the implementation plan do not remain involved for the life of the contract. Having plans and processes in place to handle the transition reduces rework and decreases the likelihood of client dissatisfaction and provider inability to perform services as expected [Ambrose 01].

SourceNet Solutions identifies five pitfalls and solutions that address the majority of problems that can occur during the first year of an outsourcing relationship [SourceNet]:

1. Inadequate knowledge transfer: Hold regular meetings to exchange information.
2. Inadequate measurement of service level performance: Establish a baseline for all negotiated service levels. Measure from the baseline and track against it, adjusting as necessary.
3. Lack of response scenario planning: Identify key events and plan the response. For example, if a successful intrusion impacts operations, a plan should exist to disconnect compromised servers and services from the network. Perform scenario exercises periodically.
4. Lack of executive sponsorship and following the established plan: Hold regular transition and performance reviews that include executives from both client and provider organizations who are responsible for the client/provider relationship.
5. Lack of flexibility: Schedule a formal review to adjust service level commitments after six months of service operation and periodically (such as annually) thereafter.

Defining and executing a detailed implementation plan help to mitigate the risks of an unsuccessful implementation. Both client and provider participate in creating this plan. Each party designates a point of contact with overall responsibility and authority for that party's implementation activities [BITS 01, Section 7, p 40].

All references to "provider" include any tiered providers that support the delivery of contracted services. Where contractual restrictions preclude a direct client interface with a tiered provider, the primary provider describes how tiered provider participation is managed and verified.

Implementation Activities

The implementation phase may include activities such as [BITS 01, Section 7.1, p 40]

- requirements definition, management, and change control, starting with requirements from the RFP and SLA
- planning and resource allocation
- technical infrastructure procurement and installation
- system modifications (hardware, software, data, configuration)
- interface development
- conversion of client data from a previous service provider or from in-house systems
- training
- system testing
- establishing secure communications mechanisms (secure voice, fax, encrypted email, pager, etc.) for exchanges that are private
- a specified, continuous period of live service operation before full transition occurs
- client acceptance testing
- documentation

Implementation Plan

The Implementation Plan contains the following information [Ambrose 01]

- transition objectives and assumptions
- known issues, constraints, and risk factors
    - Consider transitioning the smallest, most well defined, least intrusive service or service feature first, gradually adding more service capability over time.
- implementation process description including
    - how provider service systems are built and tested and whether this occurs in both a non-production (test, lab) and production environment
    - the anticipated client downtime for service installation (hours, days, how scheduled, how impact minimized) and if this can be scheduled at the client's convenience
    - the existence of a trial period during which the provider offers on-site or immediate on-call support
    - presence of back-doors into service systems and the use of modems for remote access administrative purposes; whether they are disconnected or disabled when not in use
- tasks
- deliverables
- detailed schedule and milestone dates[20]
- required resources (people, hardware, software, software licenses, other)
- assigned responsibilities (named individuals)

[20] This should reflect frequent (for example, weekly) transition and performance reviews with all key client and provider stakeholders for an agreed-upon timeframe, such as the first twelve months.

- migration of personnel, assets, software licenses, client data
- requirements for service-level acceptance (refer to Practice 3)
- ongoing review, reporting, and change management process definitions
- satisfaction of business attributes, service attributes, and security practices (refer to Practices 1, 2, and 3)
    - process definitions
    - how satisfaction is demonstrated
- approaches for obtaining buy-in from client and provider stakeholders
- contingency plans in the event that the contract is not fully implemented

Implementation Phase Exit Conditions

The following conditions should exist before implementation is considered complete [BITS 01, Section 7.2, p 40-41]:

- verification that all applicable business attributes, service attributes, and security practices are in place
- verification, through user acceptance testing and live service operation, that services are functioning as expected and service agreements are met
- verification that client data has been accurately converted
- verification that system interfaces are accurate and secure
- verification that client users have been adequately trained
- verification that provider staff members involved in delivering client services have been adequately trained
- verification that all contract terms have been implemented
- verification that any software development activity (customization, enhancements) related to the implementation is complete
- verification that all documentation is clear, comprehensive, and complete
- existence of an appropriate contingency plan and exit strategy in the event the provider fails to implement and/or provide service
- existence of an appropriate communication plan for key staff members, and stakeholders in both client and provider organizations. This may include key client customers.

The client and provider negotiate a timeframe (days, weeks, months) for successful implementation. Should implementation not be successfully completed in this timeframe, the client and provider can agree to extend the time or the client can terminate the contract at no additional cost to the client.

Post-Implementation Review

The client and the provider conclude the implementation phase by conducting a post-implementation review. Both parties evaluate the implementation plan, process, and status, agreeing on significant exceptions and documenting them. Client and provider identify open issues, assign resolution and management responsibility for issue closure and communication, and set resolution timeframes.

Practice 5: Managing an Ongoing MSS Provider Relationship

This practice contains guidelines to manage a relationship between a client and a managed security services provider after the implementation phase (Practice 4). "Planning for contract and relationship management gets overlooked. Gartner recommends that enterprises budget between three percent to eleven percent of the value of the deal for ongoing contract and relationship management [Ambrose 02]." Outsourcing relationships change over time, driven by both business changes (acquisitions, organizational responsibility shifts, business growth or contraction, regulatory changes, etc.) and technology changes (application and operating system upgrades, hardware changes, network and other technology changes, security issues, etc.) [BITS 01, Section 8, p 42]. A client needs to take these factors into account when managing the client/provider relationship.

All references to "provider" include any tiered providers that support the delivery of contracted services. Where contractual restrictions preclude a direct client interface with a tiered provider, the primary provider describes how tiered provider participation is managed and reviewed.

All client and provider responsibilities have been negotiated as part of the contract and service level agreement (refer to Practice 3).

Notifications

The provider is responsible for providing the following notifications to the client in a timely manner [BITS 01, Section 5.2, p 26; Section 5.13.3, p 3]:

- impending cessation of its business or that of a tiered provider and any contingency plans in the event of notice of such a failure (refer to Practice 6)
- financial difficulty that may impact service delivery
- significant changes in tactical or strategic decisions regarding the purchase and support of hardware or software related to service processing
- significant staffing reductions or changes in key staff that may affect the provider's ability to provide the agreed-upon support and service
- a decision to outsource, sell, or acquire significant operations or support associated with the applications, data, network, or other critical component of the environment used to provide client services
- pending press releases on any subject that may impact the client

Notification of problems or any other sensitive exchange should be conducted using secure communication mechanisms.

Ongoing Status Reviews

The client and provider review the status of their relationship, transition activities, and the provider's performance periodically (e.g., in conjunction with SLA timeframes) and as significant changes occur (e.g., rate increases). It is recommended that reviews be held weekly for the first six to twelve months of the relationship.

The client ensures that staff members representing all business unit interests are involved in overseeing the relationship and actively participate in all reviews. Client staff roles, responsibilities, and authority are clearly defined. During implementation planning (Practice 4), the client determines if there is a need to establish a steering committee that meets regularly to review open issues and report to client and provider senior management. [BITS 01, Section 8.1, p 42]

Ongoing status reviews may include the types listed below.

- Report reviews: The client regularly reviews all reports produced by the provider based on negotiated report frequency, content, format, delivery mechanism, and protection procedures. If any reports raise issues or concerns, the client contacts the provider for further discussion and resolution.

  Candidate reports may include

  - real-time network and system security status (often available as a secure web interface), a prioritized list of security alerts, and other security event reports
  - reports for specific network segments and devices, used for in-depth analysis; or reports for segment/device groups, used for overall trend analysis
  - the history and schedule for maintenance on service systems, describing maintenance actions completed as well as those still scheduled This report includes change control information as well as backup status.
  - log file information sorted and filtered to present results that meet client requirements
  - change control information reporting all service system changes over the reporting period
  - information on new security threats including those that may require changing a policy, procedure, process, or practice
  - reports useful in performing trend analysis, performance planning, and capacity planning
  - reports that verify provider compliance with contractual obligations, for example [BITS 01, Section 4.1, p 20]
    - accuracy of charges and invoices including assurance and demonstration that the client has not been billed for another client's use of provider resources [Alner 01]
    - analysis of the provider's performance in using resources to provide efficient and cost-effective services

- Service level reviews
  Upon receipt of negotiated service level reports, the client verifies that the SLA has been met in all areas for the performance period. Performance areas may include
    - service availability
    - service responsiveness
    - service security
    - infrastructure uptime or downtime
    - network performance
    - scalability
    - reporting
    - client satisfaction
    - client's customer satisfaction
    - overall end-to-end performance of service features

  This review may also include benchmarking other providers' service performance as well as their costs to ensure that the provider remains within a competitive range. The contents of SLAs can be renegotiated during these reviews, assuming this has been agreed upon.

  Provider-reported service level measurements need to be checked and correlated with the client's own measurements. All measurements should be available for independent auditing.

  Review the provider's performance monitoring and measurement tools to reconfirm their acceptability. To review end-to-end service performance, consider running sample transactions or test cases that are representative of those handled by the service. [Hiles 02]

  If service delivery performance has exceeded negotiated standards, the client enforces bonus clauses. If service delivery performance has failed to meet negotiated standards, the client enforces penalty clauses. Service level review can also be accomplished by contracting with a non-competitive third party organization to perform service level management.

- Compliance reviews
  The client periodically reapplies all proposal evaluation and selection criteria and processes to verify that the provider is still compliant. This can also be accomplished by contracting with a non-competitive third party organization to conduct a compliance review and to test all contracted services.

- Independent evaluations
  Periodically, perhaps in concert with an annual review, the client may choose to conduct (or outsource) an independent evaluation of the provider's site and services. The selection and use of independent evaluators should be mutually acceptable. A written agreement between all parties grants evaluation permission and specifies that the evaluator may not disclose any proprietary information from the provider or the client.

The client gives the provider advance notice and details of the review's scope to minimize any impacts to availability, service levels, client satisfaction, and the like. The client shares results with the provider within a specific time frame after an evaluation is performed. The client and the provider discuss any items that they mutually decide need to be resolved and they develop plans and procedures to address any changes suggested by the evaluation. [BITS 01, Section 4.1, p 20]

- Review of resolution plans and priorities for issues identified during recent
    - third-party audit reports
    - security risk evaluation reports, performed by a third party or by the provider
    - vulnerability assessments and penetration test results, performed by a third party or by the provider
    - client satisfaction survey results, performed by a third party, by the provider, or by the client

Change Management

An effective change management process is required to successfully manage and implement changes in all aspects of the relationship and all delivered services. The client verifies that the provider has a process in place to identify and assess risks resulting from change (as well as mitigation solutions) in business attributes, service attributes, and security practices (refer to Practice 1) [BITS 01, Section 8.1, p 42]. Depending on the scope of the change, many of the same activities and assessments used during proposal evaluation (Practice 2) and implementation (Practice 4) are employed during this phase, requiring close coordination between the provider and the client.

The provider should be responsive to client requests for changes, especially in the case of changes to service system infrastructure or configurations brought on by service agreements. It is critical that any changes associated with the delivery of the service be properly assessed to determine if the change presents new exposures. "For example, an upgrade to an operating system could present new vulnerabilities to intruder attacks, or a new release of an application could result in an inadvertent weakness in application security or logging." [BITS 01, Section 8.1, p 42]

Annual Review

In addition to taking actions as a result of change, perform a comprehensive review annually. It serves as additional insurance against undocumented changes and as an opportunity to evaluate the risk associated with the outsourced service.

This review can help the client determine if additional due diligence, security processes, or practices are required. The client validates that the provider has processes in place to ensure changes are documented, authorized, and approved, and that regular maintenance is performed on critical service components. The annual review takes into consideration all negotiated business attributes, service attributes, and security practices.

This review includes the following topics [BITS 01, Section 8.2, p 42-43]:

- validation of the ongoing business objectives and the necessity for outsourcing
- verification that the provider has complied with all negotiated business attributes, service attributes, and security practices and that performance is consistent with expectations
- a high-level review of all processes
- an analysis of the financial condition of the provider
- a review of recent third-party audit reports, such as SAS 70 – Type II results
- a review of recent security risk evaluation reports, performed by a third party or by the provider
- a review of recent vulnerability assessments and penetration test results, performed by a third party or by the provider
- a review of recent client satisfaction survey results, performed by a third party, by the provider or by the client
- a review of configuration change control records
- verification that supporting documentation (such as user requests) are in the appropriate files with the appropriate authorizations
- a review of the provider's service continuity, operational recovery, and disaster recovery test results; verification that the test results meet their objectives
- results from recently conducted response scenario exercises (refer to Practice 4)
- verification of maintenance on critical service assets such as key applications and security systems (for example, firewalls and intrusion detection systems)
- verification of key contacts for emergencies or to escalate critical issues
- a fully documented service description
- a full inventory and configuration report for servers, routers, any other hardware, as well as software involved in service delivery, along with supporting documentation. The provider indicates which of these the client owns and which are owned by the provider. [Berkman 01]
- service system configurations, including any files specific to the service (such as firewall rule sets, IDS signatures)
- results from "external benchmarking of 'best-of-breed' suppliers to reset prices and services levels" [Lacity 02] or to consider renegotiating these terms

The annual review includes a review of the processes used for managing service levels including [BITS 01]:

- measurement tracking and reporting
- business continuity, operational and disaster recovery
- problem escalation and dispute resolution guidelines
- service change requests including renegotiating service measurement terms
- implementing new services and service levels
- approval process
- service level review process

Review of Tiered Providers

Subject to negotiated agreements, the client reviews the performance of tiered providers using the same reports and reviews as those employed for the primary provider.

Practice 6: Terminating an MSS Provider Relationship

All outsourcing contracts must anticipate the eventual termination at the end of the contract and plan for an orderly in-house transition or a transition to another provider. Gartner research shows that outsourcing contracts terminate early more frequently than expected and under circumstances that were not anticipated. Clients and providers must jointly develop an exit strategy that defines the key resources, assets, and process requirements for continued, effective delivery of the services formerly provided by the outgoing provider. The provider is obligated to ensure that the transition happens smoothly and that the continued successful execution of services is assured. [Terdiman 01]

During contract negotiation, ensure that the contract includes a detailed description of what constitutes normal contract completion as well as early termination. Termination can occur under the following circumstances:

- termination for causes such as a breach of contract, the inability to perform, or serious breaches of security (confidentiality, integrity, availability)
- convenience
- provider insolvency or bankruptcy
- change of provider business ownership or control (for example, as a result of a merger or acquisition)
- responsibilities and services performed by the primary provider shift to a tiered provider

Use the guidelines in Practice 4 as a checklist to help review all outgoing provider transition responsibilities. Interpret these guidelines from the perspective of transitioning services from one provider to another.

Outgoing Provider Responsibilities

The outgoing provider

- notifies the client of impending cessation of its business or that of a tiered provider (for example, as a result of bankruptcy) and any contingency plans in the event of notice of such a failure [BITS 01, Section 5.13.3, p 34]. This includes
    - immediate transfer of any previously escrowed assets and data
    - providing client access to provider facilities to remove and destroy client-owned assets and data

  See also P3.2.1 Viability for other events that trigger client notification and possible contract termination.
- takes all necessary actions to ensure a smooth transition of service with minimal disruption to the client
- provides a fully documented service description
- performs and documents a gap analysis by examining the differences between its monitoring tools and those of its successor [Berkman 01]

- provides a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation. The outgoing provider indicates which of these are owned by the client and which are owned by the provider. [Berkman 01]

The outgoing provider transfers

- all assets involved in service delivery, assuming these are client-owned. For provider-owned assets, the transfer is carried out based on contract negotiations.
- all data that belongs to the client and all client-relevant data that belongs to the provider, assuming this has been negotiated

When client-owned systems have been used to deliver service, the outgoing provider transfers

- service system configurations, including any files specific to the service (such as firewall rule sets, IDS signatures)
- historical data about configuration management, including maintenance logs, if it affects service transfer

Where the outgoing provider retains ownership for service application source code, the provider follows the terms in the service level agreement (refer to P3.2.9 Exit Strategy). The provider also grants copyright release on all information and documentation required to successfully transfer service.

The outgoing provider is likely to have proprietary information about the client's systems, operations, and business. The client and outgoing provider need to determine how the provider will destroy and remove this sensitive information from all media, ensuring that it is not disclosed to other individuals or organizations. It may be necessary to either re-sign or initiate a non-disclosure agreement, requiring the provider to be thorough and complete in their efforts to ensure that no information is retained. This effort, in part, invokes a provider system discard process that eradicates all client data from disks, memory, and all other media prior to disposal.

Service Transition Timeframe

When client-owned systems have been used to deliver service, then the transition from the outgoing provider to the incoming provider is usually performed over a two-week period (though this can be negotiated). This ensures that the incoming provider has sufficient knowledge and understanding to assume service duties without interruption. The outgoing provider is obligated to provide technical support for an additional period of time, (also usually two weeks) to ensure a successful transition.

When outgoing provider-owned systems have been used to deliver service, then describe how the outgoing provider will transition the knowledge and configuration information about the current system to the incoming provider. The incoming provider needs to obtain configuration and operational information, and also needs outgoing provider support to build and test a system that duplicates the configuration of the current service system(s).

The duration of this support timeframe depends on the number of systems to be transitioned and their complexity.

The outgoing provider works closely with the incoming provider to ensure a successful transition to the new equipment, with minimal downtime and impact to the client. This work is coordinated and performed well in advance of the formal, final transition date.

Identify and document specific service tests and scenarios. Their successful execution signals the end of the transition process from the outgoing provider to the incoming provider.

Exit Clauses

Ensure the contract addresses the following topics in exit clauses:

- provider responsibilities
- client responsibilities
- the client's right to recover its data
- legal implications of termination for cause including arbitration options
- termination fees

The contract may also include provisions for the client to work directly with any tiered providers of the outgoing provider, depending on whether or not these agreements were previously established or subject to the outgoing provider's acceptance of such a working relationship.

Practice 7: Considerations for Network Boundary Protection as Managed Security Services

The management of firewalls, intrusion detection systems (IDSs), and virtual private networks (VPNs) constitutes some of the most common managed security services. These services can be simple or complex. A managed firewall service may begin and end with the purchase and installation of a perimeter firewall that protects the client's systems and networks that have a connection to the Internet. A managed firewall service may also expand to include deployment on internal sub-networks with differing access policies, regular configuration and rule set updates, monitoring, intrusion detection, intrusion response, and replacing older firewall technology with new technology. Similarly, IDS services may be limited to the purchase and installation of an initial, single sensor capability to detect and report intrusions or they may address full life cycle management that incorporates analysis across multiple sensors [McHugh 01]. An IDS service can be deployed both on internal sub-networks and those connected to the Internet. A managed VPN service can be provided at varying levels to ensure secure remote access across a small or large user population with differing authentication requirements and authorization rights.

Many of the considerations for engaging a MSSP to deploy network boundary protection services are covered in the general practices (Practice 1 – Practice 6). This practice includes technology-specific guidelines that should be considered when outsourcing these types of services. Each guideline is annotated with the general practice or practices where it should be considered (such as Practice 1 RFP, Practice 3 SLA).

Firewall Service

A managed firewall service can include a narrow or wide range of features, service levels, and capabilities. The client needs to determine their requirements for each feature, service level, and capability in order to meet business objectives and protect critical assets. The client and provider need to mutually determine roles and responsibilities including who makes service decisions and choices. In some cases, the client will make the decisions, but when it comes to choosing features of the service, the provider is often more knowledgeable and is therefore in the best position to make the right decision.

Service Description

Provide a detailed description of firewall services including [Cisco 01] [Practice 1 RFP]

- initial analysis, design, and implementation (to include transition and production operation)
- ongoing reassessment of the firewall configuration and infrastructure to ensure the current deployment reflects policy and requirements
- any services available to assist the client with implementing initial firewall policies

- process for analyzing and reporting of firewall log results (use, attack attempts blocked, summaries, etc.)
- service level features, such as adding new firewall rules, modifying a currently executing rule, and deleting a rule (routine or emergency) along with any limits on how often each feature can be requested and the response times for a given feature

Bandwidth/Throughput

The client specifies the steady state (sustained) and burst bandwidth/throughput requirements of the firewall. These are typically specified in megabits per second (Mbps). The provider demonstrates how the proposed solution meets these requirements and how throughput is operationally ensured and measured. [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA, Practice 5 Managing]

Rules Management

The provider manages and maintains the rules for specified firewalls. This can be performed for either internal firewalls, firewalls connected to the Internet, or both. Firewall rules should be maintained on a regular basis using a defined, repeatable process and should include the following activities:

- creation of rules
- modification of rules
- retirement of rules
- testing and validation of rule set changes
- ensuring all rules are applied to the correct interfaces on the firewall (especially when a DMZ (demilitarized zone) is present)
- correction of misapplied or contrasting rules
- creation of limited function or time-dependent rule(s)

Regular firewall rules management usually means that a small group of provider staff members are responsible for maintaining these rules, and are also responsible for documenting any rule changes. Specify how often firewall rule maintenance is performed, including under what events or conditions the rules are updated. Consider granting the provider permission to install emergency rule additions and changes under specified conditions. Make sure to specify the provider's response time to rule set change requests as part of the SLA. [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

The client needs to determine if the provider has implemented sound, industry accepted security practices and filtering guidelines for the firewall configuration and operation [Practice 2 Evaluation, Practice 4 Transition, Practice 5 Managing]. These include

- denying inbound traffic with an internal source network address
- denying all outbound traffic with a source network address that does not match an address on the internal network
- including rules to prevent firewall enumeration by probing and scanning techniques

- if there is a DMZ, all rules are applied to the correct interfaces on the firewall. Traffic on specified ports or from specified address ranges should be allowed into the DMZ via one ruleset, while traffic destined for the internal network should pass through a separate ruleset. These rulesets should apply to both the DMZ and the external Internet. Having two separate rulesets minimizes the chances of misconfiguration.
- ongoing evaluations to ensure rules properly implement inbound and outbound policies [Cisco 01]

Firewall Visibility
The client needs to determine if there is a requirement for a firewall to operate in stealth mode on the network, such that it cannot be enumerated by probing and scanning. This keeps a firewall in listen-mode only and makes its presence unknown to potential attackers. [Practice 3 SLA, Practice 5 Managing]

Monitoring (Proactive)
The provider reviews firewall logs at specified time intervals (12, 24, 48 hours, etc.), reports inconsistencies in network traffic, and recommends changes to the firewall system configuration. This is different from other monitoring options such as reactive monitoring which often only supports forensic analysis after security incidents have occurred. [Practice 3 SLA, Practice 5 Managing]

Stateful Packet Filtering
The provider configures the firewall system to perform stateful packet filtering rather than stateless packet filtering. Stateless packet filters specify network traffic accept/deny actions based on message header field content only, processing each message individually. Stateful packet filtering, also known as stateful inspection[21], maintains information about the state of a connection and messages exchanged thus far. This keeps external systems from being able to initiate connections to the protected network and provides more control and better information to make message-filtering decisions. Stateful packet filtering offers stronger security and network traffic management. [Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

Network Address Translation (NAT)
The firewall system has a publicly routable IP (Internet protocol) address, while all systems behind the firewall have non-Internet routable private addresses (such as 10.x.x.x or 192.168.x.x, etc.). This supports a maximum number of internal systems having access to the Internet using only one public IP address, thereby hiding internal system addresses from external view. In this case, the provider may need to gain a detailed understanding of the client's architecture behind the firewall in order to accurately design and configure the firewall to use NAT. [Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

[21] Check Point Software is credited with coining the term stateful inspection in the use of its FireWall-1 in 1993 per Webopedia at http://www.webopedia.com/TERM/S/stateful_inspection.html.

MSSP-Owned Firewall
A provider owns and installs the firewall that is used to protect the client's perimeter or internal sub-networks. The client avoids the cost of the firewall system (hardware and software) but may pay more for firewall system recurring costs (such as service, customer support, and maintenance). The provider's post-installation responsibilities are documented in the SLA. The provider's termination responsibilities are documented in the SLA or in the contract. [Practice 1 RFP, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing, Practice 6 Termination]

Repairs and Maintenance
In the case of either client or provider ownership of the firewall system, the provider agrees to perform on-site repairs, upgrades, and preventive maintenance if such maintenance cannot be performed remotely. This includes, for example, signature/filter rule updates, network diagnostics, equipment service, software and configuration updates, and data archival (backups, off-site storage). This may include specific service agreements (such as time to respond and time to repair). [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

Firewall System Reports
The means by which the provider delivers firewall system reports to the client can vary. Some providers offer online log and statistical reports, which provide near real-time information about firewall system performance and traffic patterns. Others offer paper-based reports, sending these to the client on a regular basis.

The provider should report the following firewall system information on a regular basis (via a secure communications channel):

- current status of the rules and configurations
- ruleset maintenance and other scheduled outages
- results of periodic testing of the ruleset and alert mechanisms
- operational outages (unscheduled)

[Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

Log Trending and Analysis
In addition to standard firewall system reports, some providers offer more detailed information analysis, which may include trending, anomaly detection, and threshold analysis.
This gives the client more detailed information about their network, and allows the client to be more informed when making decisions regarding the future of the network and the managed firewall service. [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

Intrusion Detection System Service

A managed IDS service can include a narrow or wide range of features, service levels, and capabilities. As for a firewall service, the client needs to determine their requirements for each feature, service level, and capability to meet business objectives and protect critical assets.

The client and provider need to mutually determine roles and responsibilities including who makes service decisions and choices. In some cases, this is the client but when it comes to detailed features of the service, the provider is often more knowledgeable and therefore is in the best position to make the right choice or decision.

Service Description
Provide a detailed description of IDS services including initial architecture analysis, design, implementation (to include transition and production operation), and ongoing reassessment of the IDS infrastructure. Describe your process for ongoing IDS sensor monitoring, analysis, and reporting of both IDS-detected attacks and network trend analysis [Cisco 01]. Describe the extent of detection and response services as discussed in P1.3.10 Monitoring and Auditing, and P1.3.11 Incident Management [Practice 1 RFP].

Multiple Network Sensors and Sensor Locations
The provider may install and manage a single sensor in a single location or may install many sensors located throughout the network that report their results to a central management console. Selecting an appropriate configuration depends on: (1) the network architecture and the elements to be monitored, (2) the need for narrow or broad traffic analysis and correlation, and (3) whether or not both incoming and outgoing traffic will be monitored. [Practice 1 RFP, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

Host-Based and Network-Based
The provider may install host-based IDSs, network-based IDSs, or both. Host-based IDSs only analyze traffic destined for a specific host as well as host performance and behavior. They are typically installed on the host of interest and generate log records either locally on that host or send them to a central log server or management station. Host-based intrusion detection is effective for isolating and analyzing events related to a specific host.

Network-based IDSs may have one or many collection sensors, and are concerned with the entire network or sub-network. In providing network-wide information, the sensors may produce far greater amounts of data than host-based systems. Both methods are effective. Selecting an appropriate combination and configuration depends on the client's detection and analysis needs and their requirements to protect their most critical assets. [Practice 1 RFP, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

Signature-Based and Anomaly-Based
The majority of detection systems currently in use are signature-based. These systems examine network message traffic headers and/or payloads (message contents). Incoming (and possibly outgoing) messages are compared with known patterns (signatures) to determine if a match occurs with a known type of attack. Signature-based IDSs are effective against known attacks whose patterns have been codified. They offer a level of forensics capability to the client and provider who maintain them. [Practice 1 RFP, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

Anomaly-based IDSs compare incoming (and possibly outgoing) network traffic against an established profile of "normal behavior." This profile is often difficult to maintain because what defines normal behavior at any given time can change. The IDS generates an alert when detected behavior exceeds some pre-established threshold or is otherwise inconsistent with the profile. This approach may be more appropriate for a well-defined, static network whose normal behavior can be predictably characterized. [Practice 1 RFP, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

The provider configures, regularly reviews, and maintains signatures and anomaly profiles for provider-supported IDSs. The provider describes what resources are used to identify potential changes and how often maintenance is performed on these definitions. Ideally, the provider has the capability to develop and implement signatures of the most recent attacks without having to wait for this information from a third party IDS vendor.

The provider uses a defined, repeatable process for signature and profile maintenance. Consider granting the provider permission to install emergency signature and profile additions and changes under specified conditions. The client needs to specify the provider's response time to IDS change requests as part of the SLA. [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

IDS Visibility
The client needs to determine if there is a requirement for the IDS to operate in stealth mode on the network, such that it cannot be enumerated by probing and scanning. This keeps the IDS in listen-mode only and makes its presence unknown to potential attackers. [Practice 3 SLA, Practice 5 Managing]

Monitoring (Proactive)
The client specifies acceptable levels of IDS false positives and false negatives[22] or negotiates these with the provider. The provider reviews IDS logs at specified time intervals (12, 24, 48 hours, etc.) and reports inconsistencies in network traffic and host performance. The provider recommends changes to the IDS configuration. This is distinct from other monitoring options such as reactive monitoring, which often only supports forensic analysis after security incidents have occurred. [Practice 3 SLA, Practice 5 Managing]

Throughput
The client specifies the steady state (sustained) and burst throughput requirements of the IDS. The provider demonstrates how the proposed solution meets these requirements and how throughput is operationally ensured and measured. [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA, Practice 5 Managing]

[22] An IDS false positive is an indication that a suspicious action has taken place when it has not. A false negative is the absence of an indication when a suspicious action has indeed occurred.

Repairs and Maintenance
In the case of either client or provider ownership of the IDS, the provider agrees to perform on-site repairs, upgrades, and preventive maintenance if such maintenance cannot be performed remotely. This includes, for example, signature/profile updates, network diagnostics, equipment service, software and configuration updates, and data archival (backups, off-site storage). This may include specific service agreements (such as time to respond and time to repair). [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

IDS Reports
The means by which the provider delivers IDS reports to the client can vary. Some providers offer online log and statistical reports, which provide near real-time information about IDS performance and traffic patterns. Others offer paper-based reports, sending these to the client on a regular basis.

The provider should report the following IDS information on a regular basis (via a secure communications channel):

- current status of the signature and profile configurations
- signature/profile maintenance and other scheduled outages
- results of periodic testing of signatures, profiles, and alert mechanisms
- operational outages (unscheduled)

[Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

Log Trending and Analysis
In addition to standard IDS system reports, some providers offer more detailed information analysis, which includes trending, anomaly detection, threshold, and traffic analysis. This gives the client more detailed information about their network and alerts the client to suspicious behavior that may be an early warning of an attack. [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

MSSP-Owned IDS
A provider owns and installs the IDS that is used to monitor the client's systems and networks. The client avoids the cost of the IDS (hardware and software) but may pay more for IDS recurring costs (such as service, customer support, and maintenance). The provider's post-installation responsibilities are documented in the SLA. The provider's termination responsibilities are documented in the SLA or in the contract. [Practice 1 RFP, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing, Practice 6 Termination]

Virtual Private Network Service

A managed VPN service can include a narrow or wide range of features, service levels, and capabilities. As for a firewall or IDS service, the client needs to determine their requirements for each feature, service level, and capability to meet business objectives and protect critical assets. The client and provider need to mutually determine roles and responsibilities including who makes service decisions and choices.

In some cases, this is the client but when it comes to detailed features of the service, the provider is often more knowledgeable and therefore is in the best position to make the right choice or decision.

Service Description
Provide a detailed description of VPN services including initial analysis, design, implementation (to include transition and production operation), and ongoing re-assessment of VPN operation. Include a description of [Cisco 01] [Practice 1 RFP]

- site-to-site and remote access VPN services
- VPN policy management from initial establishment to ongoing analysis, enforcement, and adjustments
- capabilities to support both on-site and remote VPN users including help desk support, on-demand download of client software, on-line help, assistance with initial setup, ongoing technical problem resolution, etc.
- service-level features such as routine and emergency user ID additions, adding new and deleting old VPN tunnels (routine, emergency), and VPN policy modifications along with any limits on how often features can be requested and response times to implement
- client options, if any, for administrative control of the network or any part of the VPN infrastructure
- software tools and techniques used to administer the infrastructure, indicating if these are available for client use
- any VPN self-provisioning tools, techniques, and processes (increasing bandwidth, adding nodes, etc.) and whether these can be used by the client to adjust service parameters

Bandwidth/Throughput
The client specifies the steady state (sustained) and burst bandwidth/throughput requirements of the VPN (typically specified as Mbps). The provider demonstrates how the proposed solution meets these requirements and how throughput is operationally ensured and measured. [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA, Practice 5 Managing]

The provider describes its procedures for maintaining VPN integrity at the level of service specified in the SLA, including details of the fault tolerance/fail over process to resolve service outages. [Cisco 01] [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA, Practice 5 Managing]

Authentication Alternatives
Effective operation of a secure VPN requires reliable, secure authentication of remote users who are attempting to gain access to the network. The provider can offer a range of authentication methods either singly or in combination, such as username/password, one time password, smart cards, public key, and biometrics. The required level of authentication strength (one factor, two factor, or more) depends on the client's remote access security requirements.

Higher security requirements for the network being accessed result in the need for stronger methods of authentication. [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

The provider describes the method for ensuring that only authorized VPN clients are obtaining the correct IP addresses (if there are filters based on address). If the filters are based on addresses, and the provider is not correctly handing out those addresses, other provider clients may be able to gain access to the primary client's network. Accurate and authorized address assignment is critical to the security of the remote access solution. Providers need to manage the address space appropriately, guaranteeing that only authorized, authenticated users are gaining access to the client's network. [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing]

All inbound VPN traffic should be treated as Internet traffic so that it can only be delivered to the specified services.

Encryption

The provider describes the technology used to implement the VPN (IPSec, PPTP, L2F, Frame Relay, etc.) as well as any current or future MPLS capability and integration of IPSec and MPLS.[23] [Cisco 01] [Practice 1 RFP, Practice 2 Evaluation, Practice 5 Managing]

Given that in most cases the VPN must support remote access for system administration, the provider describes their method for strong encryption (such as AES, 3DES[24], MD5[25], SHA[26], etc.) and confirms that the VPN solution is fully compliant with the IPSec protocol. [Practice 1 RFP, Practice 2 Evaluation, Practice 5 Managing]

Use Statistics

Providers may report on a range of VPN use statistics including the number of connections, connections by user, time of connections, and total time on the VPN (as measured by individual users, total bandwidth used by individual users, etc.). The provider indicates how often use statistics are collected and reported. This information aids the client in ensuring that they are getting the most for their VPN investment. It also reveals if any user or group of users are abusing the VPN service. [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

On-Site Repairs

In the case of either client or provider ownership of the VPN, the provider agrees to perform on-site repairs, upgrades, and preventive maintenance (network diagnostics and analysis, troubleshooting of network issues, equipment service, software upgrades, etc.)

---

[23] IPSec - Internet Protocol Security; PPTP - Port to Port Tunneling Protocol; L2F - Layer 2 Forwarding; MPLS - Multiprotocol Label Switching. For further details, see http://www.webopedia.com.

[24] Advanced Encryption Standard and Triple Data Encryption Standard. See http://csrc.nist.gov/cryptval/des.htm.

[25] Message Digest 5. See http://www.faqs.org/rfcs/rfc1321.html.

[26] Secure Hash Algorithm. See http://www.itl.nist.gov/fipspubs/fip180-1.htm.

[Cisco 01]. This may include specific service agreements (such as time to respond and time to repair). [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

Separate Service or Combined With a Firewall System
Some providers offer a package of VPN services coupled with managed firewall services. This may be an effective combination of network boundary protection services and may decrease overall costs if the client decides to outsource both of these services. Ensure that the combined firewall/VPN solution meets bandwidth and throughput requirements. [Practice 1 RFP, Practice 2 Evaluation, Practice 5 Managing]

Traffic Trending and Analysis
In addition to standard use reports, some providers offer more detailed information analysis to include trending, anomaly detection, traffic, and threshold analysis. This gives the client more detailed information about their network and allows the client to be more informed when making decisions regarding the future of the network and the VPN service. [Practice 1 RFP, Practice 3 SLA, Practice 5 Managing]

MSSP-Owned VPN
A provider owns and installs the VPN that is used to protect access to the client network. The client avoids the cost of the VPN (hardware and software) but may pay more for the recurring costs associated with operating the VPN, such as service, customer support, and maintenance. The provider's post installation responsibilities are documented in the SLA. The provider's termination responsibilities are documented in the SLA or in the contract. [Practice 1 RFP, Practice 3 SLA, Practice 4 Transition, Practice 5 Managing, Practice 6 Termination]

Practice 8: Considerations for Vulnerability Assessment as a Managed Security Service

Vulnerability assessments (VA) are coordinated activities whose purpose is to uncover security weaknesses in an organization's IT environment. These can include using

- proprietary, COTS[27], and open source tools to conduct automated scanning of known technical vulnerabilities in networked systems
- social engineering techniques to expose vulnerabilities in the security awareness and behavior of users including administrators
- manual techniques for conducting targeted testing on specific systems that may have escaped detection during automated scanning to identify undocumented or new vulnerabilities
- penetration testing that simulates methods used by intruders to gain unauthorized access to an organization's networked systems and then compromise them

There are many reasons why an organization may want to engage an MSSP to provide VA services including

- lack of specific VA technical knowledge and expertise
- insufficient staff time and resources
- seeking to benefit from an outsider's objectivity and the experience they have gained working with a wide range of clients
- a requirement for customized vulnerability reporting and corrective action
- a requirement for ongoing, regularly scheduled VA activities
- seeking an external "intruder's eye view" of the organization's security posture [Qualys]
- a requirement for independent affirmation of the client's security posture to build customer and partner confidence

There are several topics that an organization should consider before deciding to outsource vulnerability assessment services. This practice provides guidelines on what client organizations can expect and how best to proceed. Each guideline is annotated with the general practice(s) where it should be considered (such as Practice 1 RFP, Practice 3 SLA).

[27] commercial off-the-shelf

Considerations Prior to Conducting a VA

A client organization must carefully plan for any VA activity prior to the actual assessment and document the planning details. Consider the follow issues in advance:

- The assessment should be approved by the appropriate authority within the organization and undergo a thorough legal review. VA activities can introduce risks to information assets; systems can crash inadvertently, data can be destroyed or compromised, system performance and throughput can be affected, and, as a result, productivity and revenue can be affected. [Practice 1 RFP]

- Determine if the VA should be announced or unannounced. Announced VAs are conducted with the full cooperation and knowledge of the IT staff. Unannounced VAs are typically conducted with only the awareness of upper-level management. These VAs examine the security of the infrastructure as well as the responsiveness of IT staff [Klevinsky 02]. An unannounced VA generally comes with higher risk and a greater potential of encountering unexpected problems. [Practice 1 RFP, Practice 5 Managing]

- Consider the skill sets required for the VA team. Make sure that provider personnel have expertise with both the required tools and the systems that compose the client's operating environment. For example, if the client has a less popular network operating system, such as Novell or Banyan, the provider needs to have the required level of expertise. [Practice 2 Evaluation]

- Ensure that the provider conducts background and security checks on its assessment personnel. Serious and damaging consequences can result if provider personnel do not maintain standards of integrity and discretion. For example, Trojan horse and backdoor programs can be left behind for later access, data can be compromised, and the results of the VA can be released to the press. [Practice 2 Evaluation]

- Define the required scope of the assessment activity to include whether it is targeted or comprehensive. An organization may not want portions of its network to be subject to a VA. Critical production and revenue-generating systems such as e-commerce servers may be too vital to the organization to warrant the inevitable risks associated with comprehensive VAs. On the other hand, organizations need to be aware of the risk of unpatched vulnerabilities on their systems and the inherent risks of exposure and damage. [Practice 1 RFP, Practice 5 Managing]

Targeted assessments seek to identify vulnerabilities in specific systems and practices such as

- perimeter defenses of Internet-connected systems such as border routers, firewalls, DMZ public services (web server, FTP, external DNS, etc.) [28]
- remote access technologies such as dial-in and VPN
- Intranet services such as internal email, file and print services, and intraweb user workstation systems
- compliance with documented security policies, for example, ensuring users do not write down their passwords, and other common practices
- security of proprietary applications and software development code
- security of customer and partner data
- susceptibility to denial-of-service (network flooding) attacks

Comprehensive assessments are coordinated efforts that generally seek to uncover as many vulnerabilities as possible throughout an organization's IT practices and networked infrastructure.

- Determine ownership of all systems that will be subject to the VA. Some organizations lease Internet-connection equipment such as routers and CSU/DSU[29] from ISPs. If this is the case, the ISP should be notified of the impending VA. Include user systems connected to the organizational network via remote access such as personal laptops and hand-held computing devices such as personal digital assistants (PDAs). [Practice 1 RFP, Practice 5 Managing]

- Define all deliverable items required of the provider including the final report outline and contents, suggested solutions to exposed vulnerabilities, and level of provider support, if any, in patching discovered vulnerabilities. [Practice 3 SLA]

- Determine if the provider plans to conduct the VA remotely, onsite, or a combination of both. If the provider will be onsite, determine escort requirements and its effect on IT operations. [Practice 2 Evaluation, Practice 3 SLA, Practice 5 Managing]

- Determine provider requirements for special user accounts and privileges. Once special user accounts and privileges are approved and established, make sure these are set to expire after the VA is concluded. [Practice 3 SLA, Practice 5 Managing, Practice 6 Termination]

- Determine what tools the provider will use. Require a complete list of each tool's components and the assets (systems, networks, data, personnel) it will examine. Some open source and commercial tools are developed by white hat or black hat hackers and may have undocumented and undesirable side effects such as the installation of backdoors and worms. [Practice 2 Evaluation, Practice 5 Managing]

---

[28] Demilitarized Zone, File Transfer Protocol, Domain Name System
[29] Channel Service Unit/Data Service Unit

VA Activities

These depend on the scope of the VA. The following are examples of VA activities [Practice 1 RFP, Practice 2 Evaluation, Practice 3 SLA]:

- Attempted discovery of known vulnerabilities[30] in applications and operating systems (automated scanning tools are typically used)
    - Windows vulnerabilities such as Restrict Anonymous, default sharing permissions, and IIS[31] bugs
    - vulnerable implementations of BIND[32], DNS[33], Sendmail, and routing protocols
    - weak default configurations and built-in default accounts
    - weak authentication methods such as LAN[34] Manager allowed on Windows networks, and the use of Berkley R commands such as rlogin on networks
    - use of clear-text services such as Telnet, FTP[35], and POP3[36]
    - effectiveness of access control devices such as firewalls and routers
    - auditing to reveal poor passwords and excessive account privileges
    - virus definition currency across all tested systems
    - presence of unnecessary services on networked systems, particularly servers
    - effectiveness of logging, monitoring, and intrusion detection (if present)
    - weak remote administration practices for key systems such as the absence of encryption
    - dial-in vulnerabilities, discovered by using war dialing programs or other means, such as the presence of active modems on networked systems (dual-homed) and the presence of an inappropriately positioned modem bank (dial-in solution) in the architecture
    - network enumeration, mapping, and publicly available information such as using whois[37], ARIN[38], and other Internet resources to footprint an organization's network and attempting ping sweeps, traceroute[39], operating system identification, port scanning, zone-transfers, and other techniques to determine how vulnerable the network is to information gathering attacks

---

[30] Details of current vulnerabilities can be found at http://www.cert.org and http://cve.mitre.org. Information on vulnerability assessment tools can be found in the article "Vulnerability-assessment services on the rise" [Andress 02].

[31] Microsoft's Internet Information Server

[32] Berkeley Internet Name Domain

[33] Domain Name System

[34] Local Area Network

[35] File Transfer Protocol

[36] Post Office Protocol, used to retrieve email from a mail server

[37] whois is an Internet utility that returns information about a domain name or IP address. Refer to http://www.allwhois.com/ for further details.

[38] American Registry for Internet Numbers

[39] A utility that traces a packet from a computer to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes.

- conduct social engineering probes to determine user security awareness and behavior such as calling the help desk and attempting to have an account created or a password reset. Attempt other social engineering techniques against staff members.
- construct a flood of SYN[40] packets to test the infrastructure's ability to withstand a denial-of-service attack
- unauthorized access and use of network resources via wireless network connections

Post-Assessment Reporting and Consulting Options

Most providers attempt to make vulnerability reporting as concise and understandable as possible. This is preferred, since automated vulnerability scanning tools are infamous for returning reams of data—often riddled with false positives (reporting a vulnerability where one does not actually exist). These automated reports are generally excessively technical and difficult to understand. Additionally, it is often difficult to derive an effective solution to the reported vulnerability. Most providers offer technical consulting services to help address the reported vulnerabilities. Offered services may include online vulnerability knowledge bases, telephone assistance, and onsite technical assistance. [Practice 2 Evaluation, Practice 5 Managing]

Provider reporting options may include [Practice 3 SLA, Practice 5 Managing]

- online reports stored in encrypted databases accessible only to specific, authorized users using strong authentication methods
- online reports that are available for a limited time and then deleted from the server
- mitigation tracking systems that allow client IT staff members to monitor their progress in addressing reported vulnerabilities
- automated follow-on scans that update online reports in near real time (with necessary planning, approvals, and advance notification)
- derivative analysis reporting that describes how an organization's security posture is improving over time. These reports rely on long term, regularly scheduled VAs with the same provider

An organization needs to understand how the provider treats the disposition of the VA report and intermediate results. The information is sensitive so agreements and processes should be in place to protect its confidentiality. The provider should use strong encryption for the storage of this data and should have an agreed-upon schedule for its secure, documented destruction. [Practice 2 Evaluation, Practice 5 Managing, Practice 6 Termination]

VA reporting as an outsourced service is maturing and is making it easier for IT staff members to effectively analyze and use the reported results to address identified problems.

[40] The initial message sent from a client computer to establish a TCP connection to a system providing a service (the server).

Bibliography

[Alberts 01a] Alberts, Christopher, Dorofee, Audrey. *OCTAVE[SM] Method Implementation Guide Version 2.0.* Carnegie Mellon University: Software Engineering Institute, June, 2001. Information is available at http://www.cert.org/octave.

[Alberts 01b] Alberts, Christopher, Dorofee, Audrey, Allen, Julia. *OCTAVE[SM] Catalog of Practices, Version 2.0.* CMU/SEI-2001-TR-020 Carnegie Mellon University: Software Engineering Institute, October, 2001. Available at http://www.cert.org/archive/pdf/01tr020.pdf.

[Allen 01] Allen, Julia. *The CERT Guide to System and Network Security Practices.* Addison-Wesley, June 2001.

[Allen 00] Allen, Julia, et al. State of the Practice of Intrusion Detection Technologies. (CMU/SEI-99-TR-028), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000. Available at http://www.cert.org/archive/pdf/99tr028.pdf.

[Allen 97] Allen, Julia. *Security for Information Technology Service Contracts.* (CMU/SEI-SIM-03), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available at http://www.cert.org/security-improvement/modules/m03.html

[Alner 01] Alner, Marie. "The Effects of Outsourcing on Information Security." *Information Systems Security.* Auerbach Publications, CRC Press LLC, May/June 2001.

[Amaladoss 01] Amaladoss, Babu. "Managed Security Services – An Evolving Security Solution." March 8, 2001. Available at http://rr.sans.org/managed/mss.php.

[Ambrose 01] Ambrose, C. "IT Service Contracts – Transition and Transformation Plan." Gartner Commentary, 14 September 2001.

[Ambrose 02] Ambrose, Christopher, Helen Huntley. "Retain enough resources to manage outsourcing deals." ZDNet Tech Update, provided by Gartner, July 30, 2002. Available at http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2875650-1,00.html.

[Anderson 01] Anderson, Michelle. "On the Cutting Edge." Information Security Magazine, June, 2001. Available at http://www.infosecuritymag.com/articles/june01/departments_news.shtml.

[Andress 02] Andress, Mandy. "Vulnerability-assessment services on the rise." Network World Fusion, Network World, Inc., February 04, 2002. Available at http://www.nwfusion.com/reviews/2002/0204bgside.html.

[Armstrong 01] Armstrong, Illena. "Managed Security Services: Outside Providers to the Rescue." Info Security Magazine. June, 2001.

[Basel 01] Basel Committee on Banking Supervision. *Risk Management Principles for Electronic Banking*, specifically Appendix II Sound Practices for Managing Outsourced E-Banking Systems and Services. Bank for International Settlements, May, 2001. Available at http://www.bis.org/publ/bcbs82.pdf.

[Bassett 01] Bassett, Greg. "Developing a Computer Security Proposal for Small Businesses - How to Start." SANS Institute, August 8, 2000. Available at http://rr.sans.org/policy/cssb.php.

[Berkman 01] Berkman, Eric. "MSPs Say They'll Do It All for You." CIO Magazine, Nov 1, 2001. Available at http://www.cio.com/archive/110101/msp.html.

[BITS 01] *BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships, Version 3.2a.* BITS IT Service Providers Working Group, October, 2001. Available at http://www.bitsinfo.org/FrameworkVer32.doc.

[Bogart 01] Bogart, Barbara. "Beyond the Firewall: Information Security Offers Solution Providers Increased Opportunities, Additional Responsibilities." Red Siren, December, 2001. Available at http://www.redsiren.com/pdf/BeyondtheFirewall.pdf.

[Brittain 02] Brittain, K., Matlus, R. "Road Map for IT Service-Level Management." Gartner Article Top View, 28 January 2002.

[CERT 02] CERT/CC. "CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)." Carnegie Mellon University: Software Engineering Institute, June 25, 2002. Available at http://www.cert.org/advisories/CA-2002-03.html.

[Cisco 01] "Cisco AVVID (Architecture for Voice, Video, and Integrated Data) Partner Program - Security and VPN Services: Partner Verification Request for Information (RFI)." Cisco Systems, Inc., 2001. Information about the Partner Program is available at http://www.cisco.com/warp/public/779/largeent/partner/esap/secvpn.html.

[CIO 01] "Service Level Agreement," CIO.com. Available at http://www.cio.com/summaries/outsourcing/sla/index.html.

[Computel] "Managed Security Monitoring." Computel. Available at http://www.computel.com.lb/whitepapers4.htm.

[Counterpane] "Seven Question You Should Ask Your MSM Vendor." Available at http://www.counterpane.com/questions.html.

[Cramm 01] Cramm, Susan. "The Dark Side of Outsourcing." CIO Magazine, Nov 15, 2001. Available at http://www.cio.com/archive/111501/hs_handson.html

[Curtis 01] Curtis, D., Matlus, R., Scott, D. "Taking Magic and Mystery Out of End-to-End Service Levels." Gartner Research Note: Strategic Planning Assumption, 11 December 2001.

[Curtis 02] Curtis, D. "SLA Management: IS Organization and Business-Unit Roles." Gartner Commentary, 24 January 2002.

[DeJesus 01] DeJesus, Edmund. "Managing Managed Security." Information Security Magazine, January, 2001. Available at http://www.infosecuritymag.com/articles/january01/cover.shtml.

[Forrestal 01] Forrestal, Jeff and Shipley, Greg. "Vulnerability Assessment Scanners." Network Computing, January 8, 2001. Available at http://www.networkcomputing.com/1201/1201f1b1.html.

[Gassman 02] Gassman, B. "Using Metrics to Monitor a Service-Level Agreement." Gartner Research Note: Strategic Planning Assumption, 24 January 2002.

[Glaessner 02] Glaessner, Thomas; Kellermann, Tom; McNevin, Valerie. *Electronic Security: Risk Mitigation in Financial Transactions; Public Policy Issues*. The World Bank, June, 2002. Available at http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationversion3/$FILE/E-security-Risk+Mitigation+version+3.pdf

[Guardent] "Managed Vulnerability Protection Services." Guardent, Inc. Available at http://www.guardent.com/vas_overview.html.

[Hancock] Hancock, Bill. "Security Outsourcing The Righteous Way." Presentation slides available at http://fptest.exodus.net/go/drbill/index.html.

[Hiles 02] Hiles, Andrew. *The Complete Guide to IT Service Level Agreements: Aligning IT Service to Business Needs, Third Edition*. Rothstein Associates Inc., Brookfield, CN, 2002. Ordering information is available at http://www.servicelevelbooks.com.

[Hulme 01a] Hulme, George. "Security's Best Friend." InternetWeek, July 13, 2001. Available at http://www.informationweek.com/story/IWK20010713S0009.

[Hulme 01b] Hulme, George. "Us Great Caution When Choosing a Managed Security Vendor." InternetWeek, July 13, 2001. Available at http://www.internetweek.com/story/IWK20010713S0006.

[Hurwitz 02] Hurwitz Group. "Hurwitz TrendWatch Special Edition: Weekly Commentary and Analysis on the Software and Services Industries." Hurwitz Group, Inc., August 16, 2001. Available at http://www.hurwitz.com.

[Intexxia] "Security Quality of Service." Intexxia.

[ISF 01] Information Security Forum. *The Forum's Standard of Good Practice: The Standard for Information Security.* November 2001. Available at http://www.isfsecuritystandard.com/index_ns.htm.

[ISO/IEC 01] ISO/IEC 17799 *Information technology – Code of practices for information security management, First edition.* ISO/IEC 17799:2000(E). December 2001.

[ISS 01] Internet Security Systems. "How to Select a Managed Security Provider." April, 2001. Available at http://www.iss.net/support/documentation/whitepapers/market.php.

[James 02] James, Natalie. "(Still) At Your Service." Information Security, TruSecure Corporation, August 2002. Available at http://www.infosecuritymag.com/2002/aug/stillservice.shtml.

[King 01] King, Chris. "META Report: Are Managed Security Services Ready for Prime Time?" INT Media Group. July 13, 2001. Available at http://itmanagement.earthweb.com/secu/article/0,,11953_801181,00.html.

[Klevinsky 02] Klevinsky, Laliberte, and Gupta. *Hack IT Security through Penetration Testing.* Addison-Wesley, 2002.

[Klomp 01] Klomp, Jeremy. "Security Problems for Small Companies." SANS Institute, November 6, 2001. Available at http://rr.sans.org/homeoffice/sec_problems.php.

[Lacity 01] Lacity, M. and Willcocks, L. *Global IT Outsourcing: Search for Business Advantage.* John Wiley & Sons, New York, 2001.

[Lacity 02] Lacity, M. "Lessons in Global Information Technology Sourcing." *Computer*, IEEE Computer Society, August, 2002.

[Matlus 02] Matlus, R., Brittain, K. "Creating a Service-Level Agreement for the IS Organization." Gartner Research Note: Decision Framework, 21 January 2002.

[Maurer 02] Maurer, William, Matlus, Richard. "Reasons to re-compete sourcing deals." ZDNet Tech Update, provided by Gartner, June 28, 2002. Available at http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2872254,00.html

[McHugh 01] McHugh, John, Christie, Alan, and Allen, Julia. "Intrusion Detection: Implementation and Operational Issues." *Crosstalk: The Journal of Defense Software Engineering*, Vol. 14, No. 1. January, 2001. Available at http://www.stsc.hill.af.mil/crosstalk/2001/01/mchugh.html.

[Messmer, 02] Messmer, Ellen. "Cultivating Managed Security." Network World, June 10, 2002. Available at http://www.nwfusion.com/news/2002/0610apps.html.

[Miller] Miller, Matthew. "Integrating Security into Your Corporate Infrastructure." Red Siren, December 13, 2001. Available at http://www.acsac.org/2001/case/Thurs_C_1330_Miller_RedSiren.pdf.

[MSSP] Managed Security Services Portal. LURHQ Corporation. Available at http://www.lurhq.com/mssp.htm.

[Navarro 01] Navarro, Luis. "Information Security Risks and Managed Security Service." *Information Security Technical Report, Vol 6, No. 3*, Elsevier, 2001.

[Nicolett 02] Nicolett, M., Matlus, R. "SLAs With Outsourcers May Provide Less Than You Realize." Gartner Commentary, 21 January 2002.

[NM 01] Network Magazine India. "Crafting the Service Level Agreement." India Express Group, 2001. Available at http://www.networkmagazineindia.com/200111/focus1.htm

[Ott 01] Ott, Jeffrey L. "Managed Security Services." *Information System Security*, Vol 10, No 4, September/October 2001.

[Paquet 02] Raquet, Raymond, Nicolett, Mark. "Plan an exit strategy before signing outsourcing contracts." ZDNet Tech Update, provided by Gartner, July 30, 2002. Available at http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2875660,00.html.

[Parkhouse 02] Parkhouse, Jayne. "May 2002 Market Survey: Security Outta Site." Info Security Magazine, 2002. Available at http://www.scmagazine.com/scmagazine/2002_05/survey/survey.html.

[Pescatore 00] Pescatore, J. "Critical Security Questions to Ask an ASP." Gartner Research Note DF-10-0972, 9 February 2000.

[Pescatore 01a] Pescatore, J., Kavanagh, K., Stiennon, R. "Surviving the Managed Security Services Shakeout." Gartner Research Note, 15 March 2001.

[Pescatore 01b] Pescatore, J. "Choosing a Managed Security Services Provider." Gartner Research Note, 31 August 2001.

[Pescatore 01c] Pescatore, J. "Critical Security Questions for the Virtual Enterprise." Gartner Commentary, 19 December 2001.

[Pescatore 02] Pescatore, J. "Managed Security Services Provider Magic Quadrant." Gartner Research Note, 01 February 2002.

[Phifer 00] Phifer, Lisa. "Outsourcing Security Needs to a Managed Security Service Provider." SearchSecurity.com, November 8, 2000. Available at http://searchsecurity.techtarget.com/onlineEventsTranscript/0,289691,sid14_gci511332,00.html.

[Ploskina 01] Ploskina, Brian. "Security firms asleep at the firewall." Interactive Week. July 8, 2001.

[Qualys] "Managed Vulnerability Assessment A Proactive Approach to Network Security." Qualys, Inc. Available at http://www.qualys.com/docs/wp_mva.pdf.

[Radcliff 00] Radcliff, Deborah. "Sizing Up Security Services." Computerworld, Nov 27, 2000. Available at http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54345,00.html.

[Radcliff 01] Radcliff, Deborah. "Wanted: A Clear View of Vulnerability." Computerworld, Sep 09, 2002. Available at http://www.computerworld.com/securitytopics/security/story/0,10801,73994,00.html.

[Raffoul 02] Raffoul, Wissam. "The road to outsourcing success." ZDNet Tech Update, provided by Meta Group, March 4, 2002. Available at http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2851971,00.html.

[Red Siren] Red Siren. "Six Questions to Ask Your Managed Security Services Provider (MSSP)." Available at http://www.redsiren.com/MSSPQuestions.html.

[Scheier 01] Scheier, Robert. "Security questions to ask an ASP." December 6, 2001. Available at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci785134,00.html.

[Schneier 02] Schneier, Bruce. "The Case for Outsourcing Security." *Security and Privacy: Building Confidence in a Networked World*, Supplement to *Computer Magazine*, IEEE Computer Society, 2002. Available at http://www.computer.org/computer/sp/articles/sch/index.htm.

[SourceNet] "Change Without Pain – An Alternative Model for Year One of Outsourcing Agreements." SourceNet Solutions. Available at http://www.sourcenetsolutions.com/publications/download/outsourcing_center_white_paper.pdf.

[Stiennon 01] Stiennon, R. "Selecting a Managed IDS Service." Gartner Research Note COM-13-0815, 23 April 2001.

[Terdiman 01] Terdiman, R. "IT Services Contracts – Exit Strategy Plan." Gartner Commentary, 17 September 2001.

[Tipton 00] Tipton, Harold F., Krause, Micki. *Information Security Management, 4th Edition*, Auerbach, 2000. This book describes the International Information Systems Security Certification Consortium $(ISC)^2$ Certified Information Systems Security Professional (CISSP) Common Book of Knowledge (CBK) domain areas.

[TSS 01] TSS Publishing Team. "Why Managed Security Services?" TechSafe Solutions, 2001. Available at http://www.techsafesolutions.com/articles/why_mss.htm.

[Turek 00] Turek, Norbert. "A Safety Net for Your Web Site: Instituting the right service-level agreement can make sure vendors live up to their promises." InformationWeek.com, October 16, 2000. Available at http://www.informationweek.com/808/sla.htm.

[Verio] "Service Level Agreement (SLA)." Available at http://www.verio.com/products/managed/security/intelsec/sla.cfm.

[Wilbanks 01] Wilbanks, Joan. "Outsourcing Internet Security: The Life You Save May Be Your Company's." *Information Systems Security*. Auerbach Publications, CRC Press LLC, May/June 2001.

[Yasin 01] Yasin, Rutrell. "Enterprises Size Up Managed Security." Internet Week, June 19, 2001. Available at http://www.internetwk.com/story/INW20010619S0007.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2003	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Outsourcing Managed Security Services	F19628-00-C-0003

6. AUTHOR(S)

Julia Allen, Derek Gabbard, Christopher May

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-SIM-012

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

This report was developed by the Networked Systems Survivability Program at the Software Engineering Institute through funding from the General Services Administration Federal Computer Incident Response Center (GSA FedCIRC).

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

As computer attack patterns shift and threats to networks change and grow almost daily, it is critical that organizations achieve reliable information security. Investment decisions about information security are best considered in the context of managing business risk. Risks can be accepted, mitigated, avoided, or transferred. Outsourcing selected managed security services (MSS) by forming a partnership with a Managed Security Service Provider (MSSP) is often a good solution for transferring information security responsibility and operations. Although the organization still owns information security risk and business risk, contracting with an MSSP allows it to share risk management and mitigation approaches.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Computer Security, Outsourcing Managed Security Services (OMSS), Managed Security Service Provider (MSSP), Information Security, Risk Management	115

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18 298-102